重点大学信息安全专业规划系列教材

信息安全管理概论

胡勇 吴少华 编著

清华大学出版社

重点大学信息安全专业规划系列教材

信息安全管理概论

胡　勇　吴少华　编著

清华大学出版社
北　京

内 容 简 介

本书对信息安全管理理论与方法论做了全面的论述，也对信息安全管理的工程技术实践做了方法论的总结，包括识别信息系统及资源的方法和分类原则，识别信息系统资产的脆弱性、威胁、影响，风险分析过程描述，以及信息系统安全等级保护有关的可操作性技术方法；基于风险管理，从资源分析、风险分析与评估、安全需求分析，到安全保护策略和安全措施选择的工程实践方法和实务操作的详细描述。

本书是面向大专院校信息安全管理专业的基础教材，读者对象定位于大学计算机和通信类一级学科下的专业硕士、信息安全本科学生，以及从事信息系统管理和信息安全管理的工程技术人员。

图书在版编目(CIP)数据

信息安全管理概论/胡勇，吴少华编著. --北京：清华大学出版社，2015
重点大学信息安全专业规划系列教材
ISBN 978-7-302-39703-8

Ⅰ. ①信…　Ⅱ. ①胡…　②吴…　Ⅲ. ①信息系统－安全管理－高等学校－教材　Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2015)第 061848 号

责任编辑：付弘宇　王冰飞
封面设计：
责任校对：李建庄
责任印制：

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编：**100084
社 总 机：010-62770175　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 刷 者：
装 订 者：
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张：**14　　**字　　数：**353 千字
版　　次：2015 年 11 月第 1 版　　**印　　次：**2015 年 11 月第1 次印刷
印　　数：1～　000
定　　价：　.00 元

产品编号：060273-01

INTRODUCTION

出版说明

由于网络应用越来越普及，信息化的社会已经呈现出越来越广阔的前景，可以肯定地说，在未来的社会中，电子支付、电子银行、电子政务以及多方面的网络信息服务将深入到人类生活的方方面面。同时，随之面临的信息安全问题也日益突出，非法访问、信息窃取，甚至信息犯罪等恶意行为导致信息的严重不安全。信息安全问题已由原来的军事国防领域扩展到整个社会，因此社会各界对信息安全人才有强烈的需求。

信息安全本科专业是2000年以来结合我国特色开设的新的本科专业，是计算机、通信、数学等领域的交叉学科，主要研究确保信息安全的科学和技术。自专业创办以来，各个高校在课程设置和教材研究上一直处于探索阶段。但各高校由于本身专业设置上来自于不同的学科，如计算机、通信和数学等，在课程设置上也没有统一的指导规范，在课程内容、深浅程度和课程衔接上，存在模糊不清、内容重叠、知识覆盖不全面等现象。因此，根据信息安全类专业知识体系所覆盖的知识点，系统地研究目前信息安全专业教学所涉及的核心技术的原理、实践及其应用，合理规划信息安全专业的核心课程，在此基础上提出适合我国信息安全专业教学和人才培养的核心课程的内容框架和知识体系，并在此基础上设计新的教学模式和教学方法，对进一步提高国内信息安全专业的教学水平和质量具有重要的意义。

为了进一步提高国内信息安全专业课程的教学水平和质量，培养适应社会经济发展需要的、兼具研究能力和工程能力的高质量专业技术人才。在教育部相关教学指导委员会专家的指导和建议下，清华大学出版社与国内多所重点大学共同对我国信息安全人才培养的课程框架和知识体系，以及实践教学内容进行了深入的研究，并在该基础上形成了“信息安全人才需求与专业知识体系、课程体系的研究”等研究报告。

本系列教材是在课程体系的研究基础上总结、完善而成，力求充分体现科学性、先进性、工程性，突出专业核心课程的教材，兼顾具有专业教学特点的相关基础课程教材，探索具有发展潜力的选修课程教材，满足高校多层次教学的需要。

本系列教材在规划过程中体现了如下一些基本组织原则和特点。

(1) 反映信息安全学科的发展和专业教育的改革,适应社会对信息安全人才的培养需求,教材内容坚持基本理论的扎实和清晰,反映基本理论和原理的综合应用,在其基础上强调工程实践环节,并及时反映教学体系的调整和教学内容的更新。

(2) 反映教学需要,促进教学发展。教材要适应多样化的教学需要,正确把握教学内容和课程体系的改革方向,在选择教材内容和编写体系时注意体现素质教育、创新能力与实践能力的培养,为学生知识、能力、素质协调发展创造条件。

(3) 实施精品战略,突出重点。规划教材建设把重点放在专业核心(基础)课程的教材建设上;特别注意选择并安排一部分原来基础比较好的优秀教材或讲义修订再版,逐步形成精品教材;提倡并鼓励编写体现工程型和应用型的专业教学内容和课程体系改革成果的教材。

(4) 支持一纲多本,合理配套。专业核心课和相关基础课的教材要配套,同一门课程可以有多本具有各自内容特点的教材。处理好教材统一性与多样化,基本教材与辅助教材、教学参考书,文字教材与软件教材的关系,实现教材系列资源的配套。

(5) 依靠专家,择优落实。在制定教材规划时,依靠各课程专家在调查研究本课程教材建设现状的基础上提出规划选题。在落实主编人选时,要引入竞争机制,通过申报、评审确定主编。书稿完成后认真实行审稿程序,确保出书质量。

繁荣教材出版事业,提高教材质量的关键是教师。建立一支高水平的、以老带新的教材编写队伍才能保证教材的编写质量,希望有志于教材建设的教师能够加入到我们的编写队伍中来。

重点大学信息安全专业规划系列教材

联系人:魏江江 weijj@tup.tsinghua.edu.cn

FOREWORD

前言

这是一本面向大专院校信息安全管理专业的基础教材，读者对象定位于大学计算机和通信类一级学科下的专业硕士、信息安全本科学生，以及从事信息系统管理和信息安全管理工作的工程技术人员。

本书的作者曾在2004年承担由国务院信息化工作办公室下达的“信息安全管理指南”研究项目，此后十年来作者与同事们在信息安全本科和专业硕士的教学中结合项目的研究成果致力于对信息安全管理理论和工程实践进行与时俱进的探索，获得了一些新的知识与研究成果，在此基础上编撰成本书，以此奉献给国内从事信息安全教学与信息安全管理的朋友们。虽然作者尽了最大努力，并力求在书稿中体现中国特色和国家对信息安全管理的方针政策，但由于信息安全问题随着信息化的发展不断出现新情况，有的情况符合预期，有的情况则需要继续审视，加之作者的视野和水平所限，书中仍存在需要探索和商榷，甚至错误的地方；更由于作者在信息安全管理理论和方法研究方面的视角可能与国内同行有所不同，因此本书中如有与他人观点和管理实践不一致的地方，则应该是可以在学术上争鸣的见仁见智的事情；但作者和同事们将尽最大努力，与国内同行们继续努力，虚心学习他们的研究经验和成果，以矫正、丰富和完善我们在这一领域的研究和实践。我们希望，现在呈现给读者朋友的这本书能对读者朋友们系统地认识信息安全管理中的问题有所帮助。

本书既对信息安全管理理论与方法论有较为全面的论述，也对信息安全管理的工程技术实践做了方法论的总结，其中涉及的内容有识别信息系统及资源的方法和分类原则，识别信息系统资产的脆弱性、威胁、影响，进行风险分析的过程描述，以及与信息系统安全等级保护有关的可操作性技术方法；从信息安全管理角度进行基于风险管理的从资源分析、风险分析与评估、安全需求分析到安全保护策略和安全措施选择的工程实践方法和实务操作的详细描述。

本书由胡勇、吴少华编写，其中胡勇负责设计全书的结构，并编写第1、3、6章，吴少华编写第2、4、5章以及附录。

本书的编撰得到了戴宗坤、罗万伯两位老师的热情鼓励和直接指导，在此表示衷心的感谢。

本书的配套课件可以从清华大学出版社网站 www.tup.com.cn 下载，关于本书及课件使用的任何问题请联系 fuhy@ tup.tsinghua.edu.cn。

编　者

2015 年 10 月

CONTENTS

目录

CHAPTER 1

第1章 引言

1.1 背景

我国的信息化建设正处在蓬勃发展时期，各种基于互联网的信息化应用如雨后春笋不断涌现；各种组织或机构出于管理和业务流程的需要已经或正在建设自己的网络信息系统，这些信息系统或为组织业务提供自动化、数字化、网络化管理的技术支持和决策辅助，或为社会提供信息服务，或为个人、团体提供交流平台，等等，由此催生出一大批新兴产业。由于网络信息系统的高度互连互通性和其技术标准的开放性，对安全性的考虑不足，以及存在各种各样的威胁，使信息系统面临信息泄露、篡改，身份被假冒，网络活动被监控，甚至数据、组件、系统被损或被毁等风险，从而导致有形无形的资产损失或系统故障、瘫痪直至崩溃。这些问题就是信息安全问题，由此而伴生的另一个问题就是信息系统的安全保障问题。

信息系统安全保障是一个很广泛的概念，本书重点从管理角度就开放互连网络环境下的信息系统的安全保障问题进行系统论述，包括信息系统在设计、开发、实施、运行和维护直至报废的整个生命周期的安全保障问题，给出解决问题的管理原则和工程方法，目的在于确保信息系统在国家法律法规框架内的安全、有序和健康的运行。

为叙述方便，本书对信息系统安全和信息安全的概念不做特别区分，同理对信息系统安全保障和信息安全保障也不做特别区分。但是信息安全保障和信息系统安全保障是有区别的，前者是一个更大范围的概念，后者被包含在前者中。

信息系统安全保障涉及保护信息与系统和对抗敌对威胁这两方面的高技术综合应用。在这一应用过程中又要求将技术措施和法律性的行政管控手段结合起来。《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27 号文)明确规定，国家对信息安全保障工作的基本原则是“立足国情，以我为主，坚持管理与技术并重；正确处理安全与发展的关系，统

筹规划，突出重点，强化基础性工作；明确国家、企业、个人的责任和义务；充分发挥各方面的积极性，共同构筑国家信息安全保障体系。”科学的信息安全管理方法与实践对于信息安全保障的贡献在于两个方面，一是通过管理将信息安全技术转化为信息安全保障能力，二是以管理优势弥补技术的不足和缺失，全面优化和提升信息安全保障能力。

1.2 目的和范围

本书针对计算机网络信息系统在开放互连网络环境下的安全管理问题给出指导性的原则和工程方法，包括从管理角度对规划、设计、开发、实施、运行和维护信息系统的安全问题的识别到确保信息系统的运行始终处于安全、健康、有序和可控的状态所涉及的技术和非技术的方法和原则，以供各类信息系统在规划、设计、开发、施工和运行维护过程中参考。

1.3 适用性

本书关于信息安全管理的技术和非技术的工程方法和原则主要适用于开放系统互连网络环境下的各类信息系统，包括计算机网络信息系统和公用通信网络系统等，以及与信息技术有关的网络基础设施。

1.4 本书结构

本书共 6 章，第 1 章是引言；第 2 章为本书直接引用的基本术语和定义(依其在本书中首次出现的顺序排列)以中文形式给出，同时给出相应的英文单词或词组；第 3 章是信息安全管理概述；第 4 章为信息安全管理和组织结构；第 5 章是信息管理方法与过程；第 6 章为信息安全管理的实施。附录部分给出了与本书内容有关的名词和术语(以英文字母升序排列，同时给出相应的中文单词与词组)的词条性释义，以及英文缩略语的全称和对应的中文名词或术语。

1.5 习题与思考题

1. 查找并阅读中办发[2003]27 号文件，深入理解其中关于安全与发展的关系、统筹规划和突出重点的论述。
2. 说明信息安全管理与信息安全技术之间的关系。
3. 信息安全管理在信息系统安全保障体系中的地位和作用。

CHAPTER 2

第2章 本书直接引用的术语和定义

2.1 术语

信息技术(Information Technology,IT)

信息技术指获取、存储、加工、变换、显示和传输文字、数值、图像与视频、音频和语言信息的技术,以及提供这些技术的方法与设备的总称。这一术语有时与自动电子处理设备的含义很难严格区分。

从对信息的开发和使用角度看,信息技术可分为3个层次:第一层是硬件,主要指数据的获取、存储、处理、显示和传输的计算机和网络通信设备或组件技术;第二层是信息加工与通信软件,包括数据的获取、存储、加工、显示和传输的逻辑运算和网络通信有关的各种软件系统或模块技术,这部分技术只对开发人员可见;第三层是应用软件,指面向终端用户进行检索、查询、完成业务流程、统计分析、辅助决策等软件系统或模块技术。

信息技术安全,IT安全(IT security)

信息技术安全指获得并维持信息技术系统及其组件机密性、完整性、可用性和可控性等有关的所有方面。

信息技术安全策略,IT安全策略(IT security Policy)

信息技术安全策略指对一个组织的信息系统的所有资产(包括敏感信息在内)实施管理、保护以及分配控制措施的规则和指令。

信息安全(information security)

信息安全指保证信息和信息系统的机密性、完整性、可用性和可控性,从而使信息和信息系统免遭未授权的访问、占用、泄露、干扰、修改、重放和破坏,并保证使用和操作信息和信息系统的任何实体的身份不被假冒或欺骗、实体的来源与行为可被唯一跟踪和不可抵赖的总的特性。其中,机密性指对信息(也包括任何形式的个人隐私和专用权信息)和信息系统的访问或泄露只限于被授权者的特性;完整性指信息和信息系统不受到任何形式的未授权修改和重放的特性,还包括信息和信息系统的来源的真实性;可用性指信息

和信息系统能及时地和可靠地为授权者提供访问和使用，以及能在面对各种攻击或出现差错和故障的情况下继续提供实质性服务，并且能够及时地恢复正常服务的特性；可控性指对信息系统中出现的可预见和未预见的事件具有应对措施或应急处理预案，可控制事态的发展。

国家（信息）安全系统（National Security System）

国家（信息）安全系统指由某一（国家或政府）机构，或机构的合约方，或机构所信任的其他组织所运行或使用（包括通信基础设施在内）的信息系统。这些信息系统涉及（国家）情（谍）报活动，国计民生和社会稳定，与国家安全有关的密码活动，军事力量的指挥与控制，作为武器与武器系统组成部分的装备。

资产（asset）

资产指信息系统中对于一个组织具有价值的任何东西和事物（包括硬件的或软件的，有形的或无形的，货币化的或非货币化的，等等）。对资产的估价可采用定量、定性或定量与定性结合的计算方法。

机密性（confidentiality）

机密性指对信息和信息系统的访问和泄露只限于被授权者的特性，包括任何形式的个人隐私和专用权信息，也可理解为是信息和信息系统对未授权访问者不知其存在、不可访问（或不可接近）和不可理解的特性。

数据完整性（data integrity）

数据完整性指数据不受到任何形式的未授权修改和重放的特性，并且包括保证信息（数据）来源的真实性，其中的修改包括对数据的增加、减少、插入、生成和删除等操作行为。

完整性（integrity）

完整性是对数据完整性概念的合理延伸，指信息体和信息系统（包括软/硬件子系统和组（器）件）不受到任何形式的未授权修改和重放的特性，并且包括保证信息体和信息系统来源的真实性。完整性还适用于对连接的描述，即连接完整性。

可用性（availability）

可用性指信息和信息系统能适时地和可靠地为授权者提供访问和使用的服务能力，以及能在面对各种攻击或出现差错和故障的情况下继续提供实质性服务，并且能够及时地恢复正常服务的特性。

可确认性（accountability，又称可审查性或可追查性）

可确认性是一种保证某一实体的行为可被唯一跟踪到该实体的特性。

真实性（authenticity）

真实性是保证一个实体或资源的身份及来源就是其所声称的那个实体或资源的身份和来源的特性。真实性往往通过对用户、进程、协议层（例如网络层、传输层等）、系统和信息等实体的鉴别来实现。

抗抵赖性（non-repudiation）

抗抵赖性指对否认或抵赖曾经使用和操作过信息或信息系统的行为以及操作的内容进行对抗性证实的特性。

脆弱性(vulnerability)

脆弱性指一个或一组信息系统资源的弱点或缺陷。这些弱点或缺陷可能导致在规程(协议、格式等)、系统设计、系统实现、内部控制和运行等方面被敌对实体(威胁)开发和利用。

威胁(threat)

威胁指自然或人为(有意或无意)地限制、阻止、破坏信息系统正常运营,或降低服务(处理)能力,或降低系统或设备能力的有效性,或泄漏和窃取信息和系统资产等的潜在力量、能力和战略目标的总和。威胁包括对信息和系统的机密性、完整性、可用性、可确认性和抗抵赖性等特性造成危害的所有因素。

影响(impact)

影响指不期望的事件所引起的后果,包括有形的和无形的,货币化的和非货币化的损失。

风险(risk)

风险指给定的威胁利用某一或某组(信息系统)资源的脆弱性对一个组织造成损失的可能性(概率)以及损失(影响/后果)的总和。

风险分析(risk analysis)

风险分析指识别风险的时间和空间分布及强度(或等级),以此导出防范风险的安全需求的过程。

风险管理(risk management)

风险管理指通过适当的技术和管理措施实现阻止、降低、消除、转移或接受影响信息系统资产安全性的不定因素的总过程,包括风险分析、安全需求分析、安全保护措施的选择、实现与测试、安全评估以及所有与安全有关的管理活动。

残留风险(residual risk)

残留风险指信息系统在采取安全保护措施后仍未消除的风险,对残留风险必须评估其是否可接受。

安全措施(safeguard)

安全措施也称安全保护措施,是阻止、降低、消除或转移风险的实践、程序和机制。

积极防御(Active defence)

积极防御也称主动防御,其含义是坚持用发展的思路辩证地认识和解决信息安全保护问题,主动地应对安全风险。在对信息安全风险进行充分分析和评估的基础上构造安全防护与安全监管结合的保护体系,加强预警、应急处理和灾难备份。

基线控制(baseline control)

基线控制指一个(行业)系统或组织的信息系统从安全保障工程角度建立的安全保护措施的最小集。

组织(Organization)

组织指一个机构管理下的具有共同利益和共同安全属性的业务单位或部门的总称。例如,一个企业、一个机关或一个法人单位在本书中都以组织代称,有时也称为团体或共同体。

2.2 习题与思考题

1. 理解机密性、完整性和可用性的含义。
2. 信息系统资源和资产有什么区别与关系？
3. 脆弱性和威胁有什么关系？
4. 风险管理包括哪些过程？其中涉及哪些活动内容？
5. 残留风险的含义是什么？为什么说不宜也不能完全消除残留风险？

CHAPTER 3

第3章 信息安全管理概述

3.1 信息安全管理的总体要求和基本原则

3.1.1 总体要求

按照《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号文)的精神,信息安全保障工作的总体要求概括为坚持积极防御、综合防范的方针,全面提高信息安全防护能力,重点保障基础信息网络和重要信息系统安全,创建安全健康的网络环境,保障和促进信息化发展,保护公众利益,维护国家安全。

积极防御就是要坚持用发展的思路辩证地认识和解决信息安全问题,在对信息安全风险进行充分分析和评估的基础上构造安全防护与安全监管结合的保护体系,加强预警、应急处理和灾难备份。

综合防范就是在预防、监控、应急处理、对抗和打击犯罪等环节从法律、管理、技术、人员等方面采用多层次、立体、全面的防护措施,充分发挥国家、社会、组织和个人的作用,全社会共同构筑国家信息安全保障体系。

3.1.2 基本原则

《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号文)指出,信息安全保障工作的基本原则是"立足国情,以我为主,坚持管理与技术并重;正确处理安全与发展的关系,以安全保发展,在发展中求安全;统筹规划,突出重点,强化基础性工作;明确国家、企业、个人的责任和义务,充分发挥各个方面在信息安全保障工作中的积极性"。

"增强国家综合实力,促进经济社会的发展"是信息化的根本目的,信息安全保障为信息化的发展保驾护航。将信息安全问题绝对化,或脱离发展过程的现实而盲目追求信息安全是有害的;同样,只强调信息化应用,忽视信息安全问题则是另一个极端的错误倾向,必须坚持以安全保发展,在发展中求安全的辩证思维。同样,信息安全中的技术与管理也是辩证统一

的。在强调信息安全保障工作中的高技术防护和对抗特点时必须十分重视管理的作用。科学的管理不仅贯穿信息安全保障的全过程，而且是将信息安全技术转化为保证能力的必要条件。

我国信息安全保障中的主要设备和核心技术受制于人的现实，要求我们必须充分发挥政治和制度优势，强化信息安全意识和责任心，坚持以我为主，管理与技术并重的方针。这样做，不仅能有效地在信息安全保障体系中发挥技术与管理的互补性优势，同时也是降低信息安全保障成本的可行办法。必须坚持从本地、本单位的实际出发，根据信息化发展的不同阶段和不同的安全保护目标统筹规划，保障重点，客观分析信息安全与信息化应用的阶段适应性，综合平衡安全风险和安全成本，这是信息安全保障中始终要遵循的原则。

3.2　信息安全管理的范围

3.2.1　信息基础设施

1. 全球信息基础设施

信息基础设施(Information Infrastructure)是(有线和无线)通信网络、计算(机)设备、网络互连设备、外围设备、数据存储设备、动力保障和环境设备的集合，它可以建立在国家或地区之间的广大地域、空域和海域上。

从理论上讲，全球信息基础设施不被单个机构所控制或归其所有，它的“所有权”分布于IT公司、学术单位、政府实体以及个人。因特网(Internet)就是现今使用最为广泛和主流的全球信息基础设施实例，也是全球通信网络平台，大多数对内对外通信的网络都是在这个全球信息基础设施上建立起来的虚拟网、专用网、广域网以及定制的各种网络。

但实际上，由于这样的全球性信息基础设施中的顶级(根)服务器、路由器和域名系统(DNS)的硬件设备都控制在美国及其盟友国，大多基础通信和操作规程(协议或标准、操作系统等)的制定权和修订权以及IP地址、DNS等信息资源的分配权都掌握在由美国政府控制的大型IT企业或组织手中，这就决定了它们对全球信息基础设施资源的垄断或控制地位。

2. 国家信息基础设施

国家信息基础设施(National Information Infrastructure)是一个国家用来处理其(政府的或商业的)业务的信息基础设施，同样是(有线和无线)通信网络、计算(机)设备、网络互连设备、外围设备、数据存储设备、动力保障和环境设备的集合，也可以建立在国家或地区之间的广大地域、空域和海域上。不过，从技术层面讲，国家信息基础设施只是全球信息基础设施的一个子集。

3. 区域信息基础设施

区域信息基础设施(Local Information Infrastructure)是指一个地区、行业或组织为处理其业务所建设和使用的信息基础设施。它是国家信息基础设施的一个子集。

4. 网络边界

网络边界指位于某个国家、区域和组织的物理网络设施与外部物理网络设施之间的一个区域，这个区域往往由一台或一组网络设备(交换机、路由器等)组成，这些网络设备处理不同级别的通信交换或路由信息。与因特网相连的局域网或私有网，其物理边界就在互连

网络设备处，而逻辑边界则与不同级别的信息相关。

3.2.2　信息安全基础设施

信息安全基础设施是指可为密码服务、鉴别服务和访问控制服务等提供基础性和共享性支撑的设备和系统的通称，具体指 PKI(Public Key Infrastructure，公钥基础设施)/CA(Certification Authority，证书机构)、PKI/KMI(Key Management Infrastructure，密钥管理基础设施)和 PKI/PMI(Privilege Management Infrastructure，权限管理基础设施)等各类与公开密钥和身份标识(ID)信息有关的设备和系统，通过使用数字证书，构建网络信任体系，提供支撑性的安全基础服务。这些信息安全基础设施分别(在国家统一规划和技术标准指导下按行业、系统和业务类别)以树形结构从顶(根)至下分层进行部署，将全国大一统网络按层次分类划分为众多的虚拟网络，并按信息级别和使用权限对各类信息资源进行安全有序的访问与操作使用。

CA(Certification Authority，证书机构)负责制作、分发、撤销、作废证书等管理活动。其基本元素是数字证书，数字证书上有持有者的身份标识、权限属性、密钥信息等基本数据，是网络信任体系用户的“身份证”。

KMI(Key Management Infrastructure，密钥管理基础设施)为鉴别服务和加密服务提供密钥管理，并且提供密钥恢复服务以及存取用户证书的目录。KMI 不直接提供用户所需的安全参数，而是提供被其他安全设备和技术所使用的模块和接口参数。KMI 的主要运行过程包括登记授权使用 KMI 的个体；接受个体的密钥申请；生成对称或非对称密钥；密钥的安全分发；密钥的跟踪审计；密钥泄露和丢失处理，例如删除已泄露的密钥。

由此可知，KMI 可提供 4 个方面的业务：

① 对称密钥的产生和分发；

② 支持非对称密钥以及相应的证书管理；

③ 提供目录服务；

④ 对 KMI 自身的管理。

随着电子政务系统和电子商务系统建设的不断推进，对密钥管理的需求必将不断增长和强化，KMI 技术将被不断完善并广泛应用。

PMI(Privilege Management Infrastructure，权限管理基础设施)是信息安全基础设施中的另一个重要的组成部分。PMI 的主要目的是向用户和应用程序提供权限管理服务，负责向应用系统提供与应用相关的权限管理，提供用户身份到应用权限的映射功能，提供与实际应用处理模式对应的与具体应用系统开发和管理无关的授权和访问控制机制，可以简化具体应用系统中有关安全机制的开发和维护。

PMI 作为信息安全基础设施之一，为用户指定权限属性信息，例如特权、能力和角色等，并采用 X.509 协议所规定的数据格式使用证书。PMI 通过在应用服务中使用用户权限管理支持访问控制服务。

3.2.3　基础通信网络

我国基础通信网络担负着为国家信息化提供互连互通的网络平台服务，以及为与国际联网提供高速信道服务的重任。目前比较有影响的基础通信网络如下：

- 中国科学技术网(CSTNET);
- 中国教育和科研计算机网(CERNET);
- 中国电信公用计算机互联(骨干)网(CHINANET);
- 中国联通互联网(UNINET);
- 中国移动互联网(CMNET),等等。

国家对基础通信网络的安全管理要求是在网络交换的链路层和物理层为网络的安全有序和健康运行提供公共平台服务。为此,对基础通信网络的基本安全要求是“具有防止和对抗网络病毒传播与大规模拒绝服务攻击的能力”。

3.2.4 广播电视传输网

各级政府或政府授权的机构利用有线、无线和卫星系统构成的广播电视传输网络担负着以语音、图像和数据为外在形式的公共传媒的重任,为社会提供公共信息和社会控制信息服务。

国家对广播电视传输网的安全管理要求是“对传输信道和媒体的控制,以及防止和对抗系统外的势力对传输信道和媒体的侵占、插入、篡改和干扰,确保传输网络正常运行”。

3.2.5 信息系统

1. 国家重要信息系统

国家重要信息系统是指“关系国家安全、国计民生、经济命脉、社会稳定等方面的数据相对集中的、规模较大的信息系统,其中包括受国家委托或需要受控管理的军事工业企业和研究单位的信息系统”。这些系统通常由政府或其委托的机构负责建立、运行和维护。

2. 电子政务系统

电子政务系统是指“各级政务机关为实现办公自动化、网络化、信息化而建立、运行和维护的公文流转和业务信息系统”。这些系统辅助政府实现:

① 增强为公众、其他部门和其他政府实体提供信息和服务的能力;

② 改进政府管理工作和提升政府形象,包括增强影响力,提高效率和服务质量,以及加速政府机构和管理模式的改革进程。我国的电子政务系统分为各级政府机关的政务信息系统和各级党委机关的党务信息系统,前者原则上运行于电子政务外网上,后者完全运行于电子政务内网上。

3. 电子商务系统

电子商务系统指利用互连网络平台开展商务活动的金融、物资流通和各类交易的信息系统。

4. 企事业信息系统

企事业信息系统指各类企业和事业单位利用互连网络平台或技术所建立起来的集内部办公业务和生产、管理事务以及与社会交互为一体的综合业务信息系统。

5. 其他信息系统

其他信息系统指利用互连网络平台为社会和个人提供除上述信息系统服务功能以外的信息化服务系统,例如网吧、咨询服务和各种社交网络、即时通信、公共电子邮件系统等。

3.3　安全管理在信息安全保障中的地位和作用

安全管理和安全技术是构造信息安全保障体系的两大组成部分，两者具有同等重要的地位和作用。安全技术需要安全管理来规划、设计、实施、调整和维护，安全技术的效能需要安全管理予以激活和提升；安全管理可借助安全技术实现系统化、智能化和决策科学化。安全管理和安全技术互为支持和补充。在一定的条件下，两者可以互相转化。安全管理和安全技术的最佳融合可以提高安全保障体系的功效或绩效比，降低安全成本。

3.4　习题与思考题

1. 积极防御的核心思想是什么？

2. 深刻理解安全管理与安全技术的关系。

3. 电子政务系统是怎样分类的？为什么电子政务系统要运行在两个不同的网络上？

4. 就你知道或熟悉的网络信息系统，举两个例子，将其归类到 3.2.5 节中所述的信息系统中，并说明为什么。

5. 人们常说国际互联网（Internet）是一把“双刃剑”，根据你的理解举例说明之。

CHAPTER 4

第 4 章　管理和组织机构

4.1　信息安全管理的基本问题

4.1.1　信息系统生命周期的安全管理问题

信息系统生命周期是指信息系统从规划开始到设计（包括技术开发）、实施、使用和维护直至报废的整个过程。在这一过程中系统随着其生存环境的变化不断进行更新和维护。

从安全管理角度看，信息系统生命周期可分为下面 6 个阶段。

1. 规划阶段

在此阶段，应根据国家有关信息安全的法律法规对组织的信息系统的风险进行初步估计，并在此基础上提出安全目标，制定安全方针和策略，要求在信息系统的设计和建设中从管理和技术两个方面对信息系统安全保障体系进行同步设计、同步实施。

2. 设计和开发阶段

在此阶段，按照规划阶段提出的安全目标和制定的安全方针和策略进行基于安全风险评估的安全需求分析，以此为依据对信息安全保障体系从管理和安全技术的结合上进行整体设计，并细化为详细设计方案，给出安全投入预算。在详细设计方案中必须给出系统或组件获取途径：若有功能和性能符合设计要求的系统或组件，在采购前必须对其应具备的资质进行符合规范的审查，若无符合设计要求的系统或组件，则应委托有技术开发能力和资质的企业进行定制开发，定制开发完成的产品应提交具有资质的第三方机构进行安全符合性测试方可进行列装。

3. 实施阶段

在此阶段，信息系统所在组织正式委托具有建设能力和资质的第三方企业进行安装和调试，整个施工过程应邀请具有资质的第三方进行监理，并经过第三方的风险评估和安全性测试后交付使用。

4. 运行维护阶段

信息系统进入运行维护阶段后，一方面信息安全保障体系的维护应与信息系统的维护同步协调；另一方面，要定期根据风险的变化情况对信息系统安全保障体系的功能和效能进行评估，必要时从管理和技术措施上进行调整或更新，以维持信息和系统保障需求变化后的安全保障能力。

5. 变更和反馈阶段

信息系统投入运行后并不是一成不变的，它随着业务变动和需求变更、外界环境的变更会产生新的功能、性能需求或增强已有安全功能的需求，这就需要对信息系统的某些子系统或组件重新从规划开始进入新一轮循环。遇此情况，信息安全保障体系也应从规划开始进入新一轮的循环。

6. 废弃阶段

当信息系统已完成历史使命或被新的系统替代后即进入报废阶段，安全保障体系也随即进入废弃阶段。在此阶段，除对一般的信息安全设备或组件进行报废处置外，尤其要注意对这些设备和组件中可能残留的私密信息和数据进行彻底销毁。对其中由国家专控的(软/硬件形式的)设备和组件予以清理登记后，按照国家法律法规规定的处理程序和办法进行报废处置。

4.1.2　信息安全管理中的等级保护问题

4.1.2.1　信息系统安全保护目标

信息系统安全的保护目标与所属组织的安全保护目标是完全一致的，并具有从属关系，具体表现为对信息的保护和对系统的保护。

对信息的保护是使所属组织的供直接使用的(用于业务流程的，或用于交换服务或共享目的)信息和系统运行中(用于系统管理和运行控制目的)有关信息的机密性、完整性、可用性和可控性不受到改变和破坏。也就是说，对信息的保护实际上是对实用信息、管理信息和控制信息的保护。

对系统的保护则是使所属组织用于维持运行和履行职能的信息技术系统的可靠性、机密性、完整性和可用性不受到改变和破坏。系统保护的功能有两个，一是为信息保护提供支持，二是对信息技术系统本身进行保护。

4.1.2.2　信息系统等级保护

对信息系统进行分等级的保护是体现统筹规划、积极防范、突出重点的信息安全保护原则的重大管理策略。大量实践证明，最有效和科学的信息系统安全保护方法是在维护安全、健康、有序的网络运行环境的同时，以分级的方式确保各类信息和信息系统的适度安全，这样做既符合政策规范，又满足实际需求。划分信息系统安全保护等级的基本思想和方法如下所述。

1. 涉密信息系统保护等级的划分原则

1）系统内信息的涉密程度与信息系统的保护等级确定的关系

信息系统的保护等级由系统内涉密程度最高的信息保护等级需求确定。信息系统及其信息的涉密程度越高，保护等级越高。

2）组织级别与保护等级的关系

组织的行政级别越高，保护等级越高。

3）涉密信息量与保护等级的关系

相对集中的涉密信息量越大，保护等级越高。

4）履行职能的重要性与保护等级的关系

职能与国家安全、国计民生、社会稳定的关系越大，保护等级越高。

5）业务对信息系统的依赖性与保护等级的关系

组织业务对信息系统的依赖性越高，保护等级越高。

在遵循以上原则进行分等级保护时，要对信息系统中个别信息和组件的保护等级与整个系统的保护等级以安全域划分的方法加以适当区分，不因对个别信息和组件的高等级保护要求而提高整个系统其他信息和组件的保护等级。

2. 非涉密信息系统保护等级的划分原则

1）信息系统所属组织的社会影响与保护等级确定的关系

信息系统的保护等级由系统所属组织的社会影响力或影响面确定，社会影响越大或社会影响面越广，其保护等级越高。

2）信息系统受损后对社会的危害程度与保护等级的关系

信息系统受损后造成的社会危害性越大，保护等级越高。

3）信息系统资源价值与保护等级的关系

信息系统内的资源价值越大，保护等级越高。

4）信息系统资源利用效率与保护等级的关系

信息系统内资源的利用效率越高，保护等级越高。

5）信息系统资源密集度与保护等级的关系

信息系统内资源的集中度越高，保护等级越高。

4.1.2.3 信息系统保护等级的技术标准

确定涉密信息系统和非涉密信息系统保护等级的指导原则及其安全性评估的技术准则在 GB 17859—1999(《计算机信息系统安全保护等级划分准则》)和 GB/T 18336—2001(《信息技术 安全技术 信息技术安全性评估准则》)的基本技术框架内予以规定。对于一个组织的信息系统，可以按物理和逻辑方法划分为两个或两个以上保护等级子系统。

1. 计算机信息系统的安全保护等级

国家标准 GB 17859—1999(《计算机信息系统安全保护等级划分准则》)规定了我国计算机信息系统安全保护等级确定中应该遵循的基本原则，这是进行计算机信息系统安全等级保护制度建设的基础性依据，也是进行信息安全评估和管理的重要基础。这个标准虽然并不具备技术上的可操作性，但其基本准则却是我国各类信息系统划分保护等级和确定等级保护措施的指导原则和策略根据。

此标准将计算机信息系统安全保护从低到高划分为 5 个等级，分别为用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级，高级别安全要求是低级别安全要求的超集。计算机信息系统安全保护能力随着安全保护等级的增高逐渐增强。

在该标准中，一个重要的概念是可信计算基(TCB)。TCB 是一种实现安全策略的机制，包括硬件、固件和软件。它们根据安全策略来处理信息系统主体(系统管理员、安全管理

员、用户、进程等)对信息系统客体(进程、文件、记录、设备等)的访问,TCB 还具有抗篡改的能力和易于分析与测试的结构。TCB 主要体现该标准中的隔离和访问控制两大基本特征。各安全等级之间的差异在于 TCB 的构造不同以及所具有的安全保护能力不同。

第一级　用户自主保护级

本级的计算机信息系统可信计算基通过隔离用户与数据使用户具备自主安全保护的能力。它具有多种形式的控制能力,对用户实施访问控制,即为用户提供可行的手段保护用户和用户组信息,避免其他用户对数据的非法读/写与破坏。

本级实施的是自主访问控制,即通过可信计算基定义系统中的用户和(命名用户对命名客体的)访问,并允许用户以自己的身份或用户组的身份指定并控制对客体的访问。这意味着系统用户或用户组可以通过可信计算基自主地定义主体对客体的访问权限。

从用户的角度来看,用户自主保护级的责任只有一个,即为用户提供身份鉴别。在系统初始化时,可信计算基首先要求用户标识自己的身份(如银行卡等),然后使用身份鉴别数据(如口令字符)来鉴别用户的身份,并实施对客体的自主访问控制,避免“非法”用户对数据的读/写或破坏。

在数据完整性方面,可信计算基通过自主完整性策略阻止非授权用户修改或破坏敏感信息。

第二级　系统审计保护级

与用户自主保护级相比,本级的计算机信息系统可信计算基实施粒度更细的自主访问控制。它通过登录规程、审计安全性相关事件和隔离资源等措施使用户对自己的行为负责。

本级实施的是自主访问控制和客体的安全重用。在自主访问控制方面,可信计算基实施的自主访问控制粒度是单个用户,并控制访问权限的扩散,即没有访问权的用户只允许由授权用户指定其对客体的访问权。在客体的安全重用方面,在客体被初始指定或分配给一个主体之前,或在客体再分配之前,必须撤销该客体所含信息的授权;当一个主体获得一个客体的访问权时,原主体的活动所产生的任何信息对当前主体而言是不可获得的。

从用户的角度来看,系统审计保护级的功能有两个,即身份鉴别和安全审计。在身份鉴别方面比用户自主保护级增加两点:

- 为用户提供唯一标识,确保用户对自己的行为负责;
- 为支持安全审计功能,具有将身份标识与用户所有可审计的行为相关联的能力。

在安全审计方面,可信计算基能够创建、维护对其所保护客体的访问审计记录,还为授权主体提供审计记录接口,以便记录那些主体认为需要审计的事件,并且只有授权用户才能访问审计记录。另外,本级还支持系统安全管理员根据主体身份有选择地审计任何一个用户的行为。

在数据完整性方面,可信计算基应提供并发控制机制,以确保多个主体对同一客体的正确访问。

第三级　安全标记保护级

本级的计算机信息系统可信计算基具有系统审计保护级的所有功能。此外,还提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述;具有准确地标记输出信息的能力;消除通过测试发现的任何错误。

本级的主要特征是可信计算基实施强制访问控制。强制访问控制就是可信计算基以敏

感标记为主体和客体指定安全等级。安全等级是一个二维组，第一维是分类等级（如秘密、机密、绝密等），第二维是范畴（如适用范围等）。由可信计算基控制的主体和客体仅当满足一定条件时主体才能读/写一个客体，即仅当主体分类等级的级别高于客体分类等级的级别，主体范畴包含客体范畴时，主体才能读一个客体；仅当主体分类等级的级别低于或等于客体分类等级的级别，主体范畴包含于客体范畴时，主体才能写一个客体。

敏感标记是实施强制访问控制的基础，因此系统应明确规定需要标记的客体（如文件、记录、目录、日志等），应明确定义标记的粒度（如文件级、字段级等），并必须使其主要数据结构具有敏感标记。另外，可信计算基应维护与每个主体及其控制下的存储对象相关的敏感标记，敏感标记应准确地表示相关主体或客体的安全级别。

从用户的角度来看，系统仍呈现身份鉴别和审计两大功能。可信计算基除了具有第二级的功能外，还具有以下能力：

- 确定用户的访问权和授权访问的数据；
- 接收数据的安全级别，维护与每个主体及其控制下的存储对象相关的敏感标记；
- 维护标记的完整性；
- 维护并审计标记信息的输出，并与相关联的信息进行匹配；
- 确保以该用户的名义创建的那些在可信计算基外部的主体和授权受其访问权和授权的控制。

在数据完整性方面，可信计算基还应提供定义、验证完整性约束条件的功能，以维护客体和敏感标记的完整性。

第四级　结构化保护级

本级的计算机信息系统可信计算基建立于一个明确定义的形式化安全策略模型之上，它要求将第三级系统中的自主访问控制和强制访问控制扩展到所有主体与客体。此外，还要考虑隐蔽通道。本级的计算机信息系统可信计算基必须结构化为关键保护元素和非关键保护元素。计算机信息系统可信计算基的接口也必须明确定义，使其设计与实现能经受更充分的测试和更完整的审核。本级还增强了鉴别机制，支持系统管理员和操作员的可确认性；提供可信设施管理，增强了配置管理控制，确保系统具有相当的抗渗透能力。

本级的主要特征如下：

- 可信计算基基于一个明确定义的形式化安全保护策略。
- 将第三级实施的（自主和强制）访问控制扩展到所有主体和客体。在自主访问控制方面，可信计算基应维护由可信计算基外部主体直接或间接访问的所有资源的敏感标记；在强制访问控制方面，可信计算基应对所有可被其外部主体直接或间接访问的资源实施强制访问控制，应为这些主体和客体指定敏感标记。
- 针对隐蔽信道，将可信计算基构造为关键保护元素和非关键保护元素。
- 可信计算基具有合理定义的接口，使其能够经受严格的测试和复查。
- 通过提供可信路径来增强鉴别机制。
- 支持系统管理员和操作员的可确认性，提供可信实施管理，增强严格的配置管理控制。

在审计方面，当发生安全事件时，可信计算基还能够检测事件的发生、记录审计项、通知系统管理员、标识并审计可能利用隐蔽信道的事件。

在隐蔽信道分析方面，系统开发者应彻底搜索隐蔽信道，并确定信道的最大带宽，这样才能确定有关正常使用隐蔽信道的非安全事件。

第五级　访问验证保护级

本级的计算机信息系统可信计算基满足访问监控器（Reference Monitor）需求。访问监控器判断主体对客体的全部访问。访问监控器本身具备抗篡改性，且必须足够小，能够分析和测试。为了满足访问监控器需求，计算机信息系统可信计算基在构造时，排除那些对实施安全策略来说并非必要的代码；在设计和实现时，从系统工程角度将其复杂性降低到最小。它支持安全管理员可确认性；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制，系统具有很高的抗渗透能力。

本级与第四级相比，主要区别在以下 4 个方面：

- 在可信计算基的构造方面具有访问监控器。所谓访问监控器，是监控主体和客体之间授权访问关系的部件，仲裁主体对客体的全部访问。访问监控器必须是抗篡改的，并且是可被分析和测试的。
- 在自主访问控制方面，因为有访问监控器，所以访问控制能够为每个客体指定用户和用户组，并规定它们对客体的访问模式。
- 在审计方面，在访问监控器的支持下，可信计算基扩展了审计能力。本级的审计机制能监控可审计安全事件的发生和积累。当积累超过规定的门限值时，能够立即向系统管理员发出报警，并且，如果这些与安全相关的事件继续发生，能以最小的代价终止它们。
- 在系统的可信恢复方面，可信计算基提供了一组过程和相应的机制，保证系统失效或中断后可以进行不损害任何安全保护性能的恢复。

2. 基于通用准则的安全评估保证等级

信息技术安全性评估准则（GB/T 18336：2000，等同于 ISO/IEC 15408：1999，又称通用准则（Common Criteria，CC））中定义了 7 个递增的安全评估保证级（Evaluation Assurance Level，EAL），这种递增靠替换成同一保证子类中的一个更高级别的保证组件（即增加严格性、范围或深度）和添加另外一个保证子类的保证组件（例如，添加新的要求）来实现。

评估保证级是由 GB 18336 第 3 部分中的保证组件构成的包，该包代表了 CC 通用准则预先定义的保证尺度上的某个保证要求集。一个保证级是评估保证要求的一个基线集合。每一个评估保证级定义一套一致的保证要求，合起来，评估保证级构成一个预定义 CC 保证级尺度。

评估保证级并不用于直接对信息和系统的等级保护，而是用于对信息和系统的保护有效性进行评估和验收，包括对保护措施（或保证组件）的功能和效能进行等级评估、测试和验证。

评估保证级 1（EAL1）——功能测试

EAL1 适用于对正确运行需要一定信任的场合，在该场合中安全威胁并不严重。它还适用于需要独立的保证来支持在人员或类似信息的保护方面已经给予足够重视的情况。

EAL1 为用户提供了 TOE（Target of Evaluation，评估对象）的一个评估，包括依据一个规范的独立性测试和对所提供的指导性文档的检查。在没有 TOE 开发者的帮助下，一个

EAL1 评估也能成功地进行，而且所需的费用最少。

该级别的评估应当确认 TOE 的功能与其文档在形式上是一致的，并且对已标识的威胁提供了有效的保护。

EAL1 通过功能和接口的规范以及指导性文档对安全功能进行分析，以提供一种基础级别的保证。

EAL1 通过对 TOE 安全功能的独立性测试来分析安全功能。

和未经评估的 IT 产品或系统相比，本 EAL 提供了保证的增强。

评估保证级 2(EAL2)——结构测试

在交付设计信息和测试结果时，EAL2 需要开发者的适度合作，且不需要增加过多的费用或时间的投入。

EAL2 适用于以下情况：在缺乏现成可用的完整的开发记录时，开发者或使用者需要一种低到中等级别的独立保证的安全性。在传统的保密系统或者同开发者的访问受到限制时会出现这种情况。

EAL2 通过功能和接口的规范、指导性文档和 TOE 的高层设计对安全功能进行分析以提供保证。

这种分析由以下诸因素提供支持：TOE 安全功能的独立性测试，开发者基于功能规范进行测试得到的证据，对开发者测试结果的选择性独立确认，功能强度分析，开发者搜索明显的脆弱性(如公开的脆弱性)的证据。

EAL2 也通过 TOE 的配置表和安全交付程序的证据来提供保证。

EAL2 在 EAL1 的基础上增加了保证。这是通过要求开发者测试以及在 EAL1 基础上增加脆弱性分析和基于更详细的 TOE 规范的独立性测试来实现的。

评估保证级 3(EAL3)——系统的测试和检查

EAL3 可使一个尽职尽责的开发者在设计阶段从正确的安全工程中获得最大限度的保证，而不需要对现有的合理的开发实践做大规模的改变。

EAL3 适用于以下情况：开发者或使用者需要一个中等级别的独立保证的安全性，在没有再次进行真正的工程实践的情况下要求对 TOE 及其开发过程进行彻底调查。

EAL3 通过功能和接口的规范、指导性文档和 TOE 的高层设计保证安全功能。

这种分析由以下诸因素提供支持：TOE 安全功能的独立性测试，开发者基于功能规范和高层设计进行测试得到的证据，对开发者测试结果的选择性独立确认，功能强度分析，开发者搜索明显的脆弱性(如公开的脆弱性)的证据。

EAL3 还通过使用开发环境控制措施、TOE 的配置管理和安全交付程序的证据来提供保证。

EAL3 在 EAL2 的基础上增加了保证，这是通过要求更完备的安全功能测试范围以及要求提供一些 TOE 在开发过程中不会被篡改的可信性的机制或程序来实现的。

评估保证级 4(EAL4)——系统的设计、测试和复查

EAL4 可使开发者从正确的安全工程开发实践中获得最大限度的保证。这种实践虽然很严格，但并不需要大量的专业知识、技巧和其他资源。在经济合理的条件下，对一个已经存在的生产线进行翻新时，EAL4 是所能达到的最高级别。

EAL4 适用于以下两种情况：开发者或使用者对传统的商品化的 TOE 需要一个中等

到高等级别的独立保证的安全性和准备负担额外的安全工程专门费用。

EAL4 通过功能规范和完备的接口规范、指导性文档、TOE 的高层设计和低层设计、实现的子集保证安全功能，也可通过 TOE 安全策略的一个非形式化模型来获得额外的保证。

这种分析由以下诸因素提供支持：TOE 安全功能的独立性测试，开发者基于功能规范和高层设计进行测试得到的证据，对开发者测试结果的选择性独立确认，功能强度分析，开发者搜索脆弱性的证据，以及对抵御低级的穿透性攻击的能力进行论证的独立脆弱性分析。

EAL4 还通过使用开发环境控制措施、包括自动化在内的额外的 TOE 配置管理以及安全交付程序的证据来提供保证。

EAL4 在 EAL3 的基础上通过要求更多的设计描述、实现的子集以及提供 TOE 在开发或交付过程中不会被篡改的可信性的改进机制或程序来增加保证。

评估保证级 5(EAL5)——半形式化的设计和测试

EAL5 可使一个开发者从严格的安全工程开发实践中获得最大限度的保证，这是靠应用专业安全工程技术来支持的。设计和开发这样的 TOE 需要有达到 EAL5 保证的决心。相对于没有应用专业技术的严格开发而言，由 EAL5 要求引起的额外开销也许不会很大。

EAL5 适用于以下情况：开发者和使用者在有计划的开发中需要一个高级别的独立的安全性保证，和在专业安全工程技术不会引起不合理开销的条件下需要一种严格的开发手段。

EAL5 通过功能规范和完备的接口规范、指导性文档、TOE 的高层和低层设计以及所有的实现提供安全功能保证，也可以通过以下方式额外地获得保证：TOE 安全策略的形式化模型、功能规范和高层设计的半形式化表示，以及它们之间对应性的半形式化论证，此外还需要一个模块化的 TOE 设计。

该级的保证来源于 TOE 安全功能的独立性测试，开发者基于功能规范、高层设计和低层设计进行测试得到的证据，对开发者测试结果的选择性独立确认，功能强度分析，开发者搜索脆弱性的证据，以及对抵御中等攻击潜力的穿透性攻击者的能力进行论证的独立脆弱性分析。这种分析也包括对开发者的隐蔽信道分析的确认。

EAL5 还通过使用开发环境控制措施、包括自动化在内的全面的 TOE 配置管理以及安全交付程序的证据来提供保证。

EAL5 在 EAL4 的基础上增加了保证，这是通过要求半形式化的设计描述、整个实现、更结构化(因而更具有可分析性)的体系、隐蔽信道分析，以及提供 TOE 在开发过程中不会被篡改的可信性的改进机制或程序来实现的。

评估保证级 6(EAL6)——半形式化验证的设计和测试

EAL6 可使开发者通过把安全工程技术应用于严格的开发环境获得高度的保证，以便生产一个昂贵的 TOE 来对抗重大的风险，保护高价值的资产。

EAL6 适用于以下情况：应用于高风险环境下的安全 TOE 的开发，在这里受保护的资源值得花费额外的开销。

EAL6 通过利用功能规范和完备的接口规范、指导性文档、TOE 的高层和低层设计以及实现的结构化表示对安全功能进行分析来提供保证，以理解安全行为。还通过以下方式获得额外的保证：TOE 安全策略的形式化模型，功能规范、高层设计和低层设计的半形式化表示，以及它们之间对应性的半形式化论证，此外还需要模块化和分层的 TOE 设计。

该级保证来源于 TOE 安全功能的独立性测试，开发者基于功能规范、高层设计和低层

设计进行测试得到的证据，对开发者测试结果的选择性独立确认，功能强度分析，开发者搜索脆弱性的证据，以及对抵御高等攻击潜力的穿透性攻击者的能力进行论证的独立脆弱性分析，还包括对开发者的系统化隐蔽信道分析。

EAL6 也通过使用结构化的开发流程、开发环境控制措施、包括完全自动化在内的全面的 TOE 配置管理以及安全交付程序的证据等来提供保证。

EAL6 在 EAL5 的基础上增加了保证，这是通过更全面的分析实现的结构化表示、更体系化的结构(如分层)、更全面的独立脆弱性分析、系统化隐蔽信道识别，以及改进了的配置管理和开发环境控制等实现的。

评估保证级 7(EAL7)——形式化验证的设计和测试

EAL7 适用于安全 TOE 的开发，该 TOE 将应用在风险非常高的地方或有高价值资产、值得更高开销的地方。EAL7 的实际应用目前只局限于一些 TOE，这些 TOE 非常关注能经受广泛的形式化分析的安全功能。

EAL7 通过利用功能规范和完备的接口规范、指导性文档、TOE 的高层和低层设计以及实现的结构化表示对安全功能进行分析来提供保证，以理解安全行为，也可通过以下方式获得额外保证：TOE 安全策略的形式化模型，功能规范和高层设计的形式化表示，低层设计的半形式化表示，以及它们之间对应性的适当的形式化和半形式化论证，此外还需要一个模块化的、分层的且简单的 TOE 设计。

该级保证来源于 TOE 安全功能的独立性测试，开发者基于功能规范、高层设计、低层设计和实现表示进行测试得到的证据，对开发者测试结果的全部独立确认，功能强度分析，开发者搜索脆弱性的证据，以及对抵御高等攻击潜力的穿透性攻击者的能力进行论证的独立脆弱性分析，还包括对开发者的系统化隐蔽信道分析。

EAL7 也通过使用结构化的开发流程、开发环境控制措施、包括完全自动化在内的全面的 TOE 配置管理以及安全交付程序的证据等来提供保证。

EAL7 在 EAL6 的基础上增加了保证，这是通过要求利用形式化表示和对应性的形式化进行更全面的分析，以及更全面的测试来实现的。

3. 几种安全等级标准的对应关系

表 4.1 给出了几种安全等级标准的对应关系。

表 4.1　几种安全等级标准的对应关系

CC	GB/T 17859	TCSEC	FC	CTCPEC	ITSEC
EAL1	—	—	—	—	—
EAL2	第 1 级	C1	—	—	E1
EAL3	第 2 级	C2	T-1	T-1	E2
EAL4	第 3 级	B1	T-2	T-2	E3
—	—	—	T-3	T-3	—
—	—	—	T-4	—	—
EAL5	第 4 级	B2	T-5	T-4	E4
EAL6	第 5 级	B3	T-6	T-5	E5
EAL7	—	A1	T-7	T-6	E6
—	—	—	—	T-7	—

表 4.1 中，CC——Common Criteria：通用准则。

TCSEC——Trusted Computer System Evaluation Criteria：可信计算机系统评估准则，由美国于 1985 年提出，在 2000 年 12 月停止使用。

FC——Federal Criteria：美国联邦准则。

CTCPEC——Canada Trusted Computer Product Evaluation Criteria：加拿大可信计算基评估准则。

ITSEC——Information Technology Security Evaluation Criteria：信息技术安全评估准则（欧洲）。

4.1.3　信息安全管理的基本内容

信息系统的安全管理涉及与信息系统有关的安全管理以及对信息系统管理的安全管理两个方面。这两个方面的管理又分为技术性管理和行政性管理两类。其中，技术性管理以对 OSI 安全机制和安全服务的管理以及对物理环境的技术监控为主；行政性管理以法律法规、规章制度的遵从性管理为主。信息安全管理本身并不执行特定的业务应用和通信过程，只是为这些业务应用和通信过程中的安全机制与安全服务提供支持与控制。

由信息系统的行政管理部门依照法律并结合本单位安全的实际需要而制定的信息系统的安全策略是信息安全管理活动的重要组成部分。受同一个机构管理并执行同一个安全策略的多个网络实体构成的集合有时称为“安全域”。安全域以及它们之间的相互关系和影响需要受到管理者的特别重视。

对信息系统管理的安全管理包括对信息系统所有管理行为和协议的安全管理，以及对信息系统管理信息的通信的安全管理，它们是信息系统安全管理的重要组成部分。这一类安全管理将借助对信息系统安全服务与机制进行适当的配置确保信息系统管理协议与管理信息的通信获得足够的保护。

在信息安全管理的技术性规范中，为了强化安全策略的协调性和安全组件之间的互操作性，特别提出一个极为重要的基本概念，即安全管理信息库（Security Management Information Base，SMIB），用于存储和交换开放系统所需的与安全有关的全部信息。SMIB 是一个分布式信息库，在实际操作中，SMIB 的某些部分可以与管理信息库（Management Information Base，MIB）结合成一体，也可以完全分开。SMIB 有多种实现方式，例如数据表、文件，以及嵌入到开放系统软件或硬件中的数据或规则。

安全管理协议以及传送这些管理信息的通信信道可能遭受攻击，所以应特别对安全管理协议及其协议数据加以保护，其保护的强度通常不低于为业务应用通信提供的安全保护的强度。

安全管理可以使用 SMIB 信息在不同行政管理机构的信息系统之间交换与安全有关的信息。在某些情况下，与安全有关的信息可经由非自动信息通信通路传递，局部系统的管理者也可采用非标准化方法来修改 SMIB。在另外一些情况下，可能希望通过信息通信通道在两个安全管理事务之间传递信息。在获得安全管理者授权后，该安全管理事务将使用这些通信信息来修改 SMIB，但是修改 SMIB 必须先得到安全管理者的授权。

4.2 信息安全等级保护的管理

为了规范全国各系统各行业的电子政务信息系统、重要信息系统、企事业信息系统在信息安全等级保护工作中的管理活动，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设，根据《中华人民共和国计算机信息系统安全保护条例》等有关法律法规，由公安部、国家保密局、国家密码管理局、国务院信息化工作办公室于2007年6月22日以公通字[2007]43号文件形式联合颁发《信息安全等级保护管理办法》(在本节的叙述中简称《管理办法》)。

对不同的信息系统实行分等级的安全保护是我国信息安全保障体系建设的一个里程碑式的战略决策，标志着我国信息系统安全保护工作向体系化、科学化的发展方向迈出了关键性的一步。分等级保护的实施将从制度上解决长期困扰人们的一个难题，即从方法论上解决了不同安全保护需求的过度保护或保护不够的问题，由此带来的社会经济利益是巨大的。

《管理办法》将信息系统安全保护等级划分为5个级别，通称为等级保护(简称等保)，等级保护的主管机构为公安机关，具体负责对信息安全等级保护工作的监督、检查、指导；按照5个保护等级的基本思想对涉密信息系统的安全保护规定了3个级别，通称为分级保护(简称分保)，分级保护的主管机构为国家保密工作部门，具体负责对涉密信息系统分级保护的工作监督、检查、指导；国家密码管理部门具体负责信息系统等级保护和涉密信息系统分级保护工作中有关密码工作的监督、检查、指导；国务院信息化工作办公室及地方信息化领导小组办事机构具体负责等级保护工作的部门间的协调。

国家各级公安机关为实施《管理办法》出台了信息安全等级保护的具体管理办法，对等级保护管理工作中涉及监督、检查和指导的具体事务做出了明确的规定。

随后由国家公安部信息安全等级保护评估中心起草的《信息系统安全等级保护定级指南》(GB/T 22240—2008)对信息系统安全等级的定级方法进行了详细描述。

国家制定的这些统一的信息安全等级保护管理规范和技术标准是我国信息系统安全保护工作的纲领性指导文献，标志着我国信息安全保障工作上了一个新的台阶，为我国各类信息系统依法保护其信息资产提供了具有可操作性的管理规范，以及可实现的技术标准，必将推动我国的信息安全保障建设更加系统化和科学化。

《管理办法》要求信息系统的安全主管部门应本着分工负责、相互协调的精神依照《管理办法》及相关标准规范，督促、检查、指导本行业、本系统或者本地区信息系统的运营、使用单位的信息安全等级保护工作；信息系统的运营、使用单位应当依照《管理办法》及其相关标准规范实施等保工作，履行信息安全等级保护的义务和责任。

近十多年来的实践证明，信息系统安全等级保护的主管部门与实施单位的良性互动和良好合作是信息安全等级保护管理工作取得成功的基础。

4.2.1 安全保护等级的划分

按照《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号文)关于“立足国情，以我为主”的原则精神，信息安全等级保护坚持自主定级、自主保护的方针。因此，信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中

的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素予以确定。从技术角度看，如果把信息安全保护等级的确定作为系统工程的输出因变量，那么它的输入就是多自变量。换句话说，信息安全保护等级的确定不太可能依赖单一因素就可以解决问题，而是需要综合考虑多种因素的影响，当然这多种因素中可能有一个或两个因素会对等级的确定起到决定性作用，这也是人们通常所说的影响因素权重的问题。

4.2.1.1　安全保护等级的框架

参照《计算机信息系统安全保护等级划分准则》(GB 17859—1999)，《管理办法》将我国信息系统的安全保护等级划分为以下 5 个等级：

第一级，信息系统受到破坏后会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后会对公民、法人和其他组织的合法权益产生严重的损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后会对社会秩序和公共利益造成严重的损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后会对社会秩序和公共利益造成特别严重的损害，或者对国家安全造成严重的损害。

第五级，信息系统受到破坏后会对国家安全造成特别严重的损害。

这 5 个等级为确定信息系统的安全保护强度提供了一个框架指导，在实际定级工作中是不可操作的。问题在于如何界定信息系统受到破坏后“会对公民、法人和其他组织的合法权益造成损害”？如何界定信息系统受到破坏后“会对公民、法人和其他组织的合法权益产生严重的损害，或者对社会秩序和公共利益造成损害，但不损害国家安全”？如何界定信息系统受到破坏后“会对社会秩序和公共利益造成严重的损害，或者对国家安全造成损害”？如何界定信息系统受到破坏后“会对社会秩序和公共利益造成特别严重的损害，或者对国家安全造成严重的损害”？如何界定信息系统受到破坏后“会对国家安全造成特别严重的损害”？

接下来的内容将回答上述问题。

4.2.1.2　安全保护等级的划分方法

1. 定级对象

从信息安全保护等级的五级框架定义出发，首先要明确给谁定级，即什么样的信息系统才是利用五级框架定级的适用对象？其次，“对公民、法人和其他组织的合法权益造成损害或严重的损害”、“对社会秩序和公共利益造成损害或严重的损害”和“对国家安全造成损害”或“严重的损害”或“特别严重的损害”等这样一些衡量信息系统需要保护的等级需求指标在哪里寻找可以观察的表现形式？

根据(GB/T 22240—2008)《信息安全等级保护的定级指南》对定级对象的定义，作为定级对象的信息系统应具有以下基本特征。

1) 具有唯一确定的安全责任单位

作为定级对象的信息系统，应该有一个机构或其所属的组织对信息系统的安全负责。

如果一个组织的某个下属机构负责信息系统安全建设、运行和维护等过程的全部安全责任，则这个下属机构可以成为该信息系统的安全责任单位；如果一个组织的不同下属机构分别承担信息系统不同方面的安全责任，则该信息系统的安全责任单位应是这些下属机构共同所属的上一级组织。

2）具有完整的信息系统的基本要素

作为定级对象的信息系统，应该是由相关的和配套的设备、设施按照一定的应用目标和规则组合而成的独立的或相对独立的有形实体。单一的系统组件，如服务器、终端、网络设备等没有必要作为定级对象。

3）承载单一或相对独立的业务应用

作为定级对象的信息系统，可以承载"单一"的业务应用（即该业务应用的业务流程独立，与其他业务应用没有数据交换），且独享所有信息处理设备（即不与其他应用程序共享其中的所有或部分信息处理设备）；也可以承载"相对独立"的业务应用（即其业务应用的主要业务流程独立，与其他业务应用只有少量的数据交换），这样的信息系统可能会与其他业务应用程序共享一些设备，尤其是网络传输设备。

对于大型组织机构内运行的信息系统而言，一般承载不止一个"单一"业务应用，信息处理设备的共享程度高（例如核心交换机、传输网络、存储区域），可将较大的信息系统划分为若干个较小的、可能具有不同安全保护等级的定级对象。每个较小的定级对象或按承载单一业务应用流程（即该业务应用的业务流程独立，与其他业务应用没有数据交换），或按承载"相对独立"的业务应用（即其业务应用的主要业务流程独立，与其他业务应用只有少量的数据交换）的方法确定。这样，既体现对重要部分的重点保护，又兼顾到一般的保护需求，不仅可以有效地控制信息安全建设成本，也能依此方法解决对一些信息资源的保护过度而对另一些信息资源的保护不足的问题，这是一种优化信息安全资源配置的科学方法。

2. 定级要素

信息系统的功能在于处理业务信息和提供服务。在对信息系统确定安全保护等级时必须确定信息系统内业务信息的安全保护等级和系统服务的安全保护等级，当这两个子系统的保护等级不相同时，则以其中较高的等级作为信息系统的安全保护等级。

但是直接考察业务信息和系统服务所需要的安全保护等级几乎是无从下手，那么是否可以通过因果关系的分析来推导出业务信息和业务服务的安全保护等级需求呢？这里可以将信息系统安全保护等级看作结论，那么信息系统安全遭受破坏后对国家和社会造成的损害以及损害的程度就是必要条件，因此只有当满足一定的条件后才能得出某一结论。在我国国情和社会制度的背景下，对信息系统安全遭受破坏后所受到的影响（被损害的国家和社会性要素，以及被损害的程度）是可以定性或定量进行评估的，这就为确定保护等级提供了可行的方法。

《信息安全等级保护的定级指南》（GB/T 22240—2008）将信息系统遭受破坏后的影响要素定义为与信息系统安全遭受破坏后相关的受侵害客体和对客体的侵害程度。由此推定，信息系统的安全保护等级由两个定级要素来决定，即等级保护对象（信息系统）受到破坏时所侵害的客体和对客体造成侵害的程度。

1）受侵害的客体

等级保护对象（信息系统）受到破坏时直接或间接地损害到客体（一些可以观测或感受

的货币化或非货币化形态的事物)，这些客体包括以下内容：

- 公民、法人和其他组织的合法权益；
- 社会秩序、公共利益；
- 国家安全。

2) 对客体的侵害程度

由于对客体的侵害是对等级保护对象(信息系统)破坏的外在表现，因此，对等级保护对象(信息系统)的破坏可以通过客体被危害的程度加以描述。

等级保护对象(信息系统)受到破坏后对客体造成侵害的程度归纳如下：

- 一般损害；
- 严重损害；
- 特别严重损害。

关于客体受到损害的 3 个程度限定副词(一般、严重、特别严重)的判断，在客观上可以设计一些观察指标(在下面的"4. 等级确定"处有详细描述)。这些指标是定性与定量相结合的综合指标体系，运用这些指标来辅助确定信息安全保护等级还需要有评估人员主观因素的配合，这些主观因素包括与确定保护等级的相关人员的技术能力、职业素质和责任心。

定级要素与信息系统安全保护等级的关系如表 4.2 所示。

表 4.2　定级要素与安全保护等级的关系

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

由表 4.2 可知，只要在对客体及其所受损害的程度确定后即可确定保护等级。

3. 定级流程

信息系统安全包括业务信息安全和系统服务安全，与之相关的受侵害客体和对客体的侵害程度可能不同，因此，信息系统定级也应由业务信息安全和系统服务安全两个方面确定。

从业务信息安全角度反映的信息系统安全保护等级称业务信息安全保护等级。

从系统服务安全角度反映的信息系统安全保护等级称系统服务安全保护等级。

确定信息系统安全保护等级的一般步骤如下：

① 确定作为定级对象的信息系统，并列出业务信息和系统服务；

② 确定业务信息安全受到破坏时所侵害的客体；

③ 综合评定业务信息安全被破坏对不同客体的侵害程度；

④ 依据表 4.3 得到业务信息安全保护等级；

⑤ 确定系统服务安全受到破坏时所侵害的客体；

⑥ 综合评定系统服务安全被破坏对不同客体的侵害程度；

⑦ 依据表 4.4 得到系统服务安全保护等级；

⑧ 将业务信息安全保护等级和系统服务安全保护等级较高者确定为定级对象的安全

保护等级。

上述步骤如图 4.1 所示，其中各项描述分别对应图 4.1 中的各项描述。

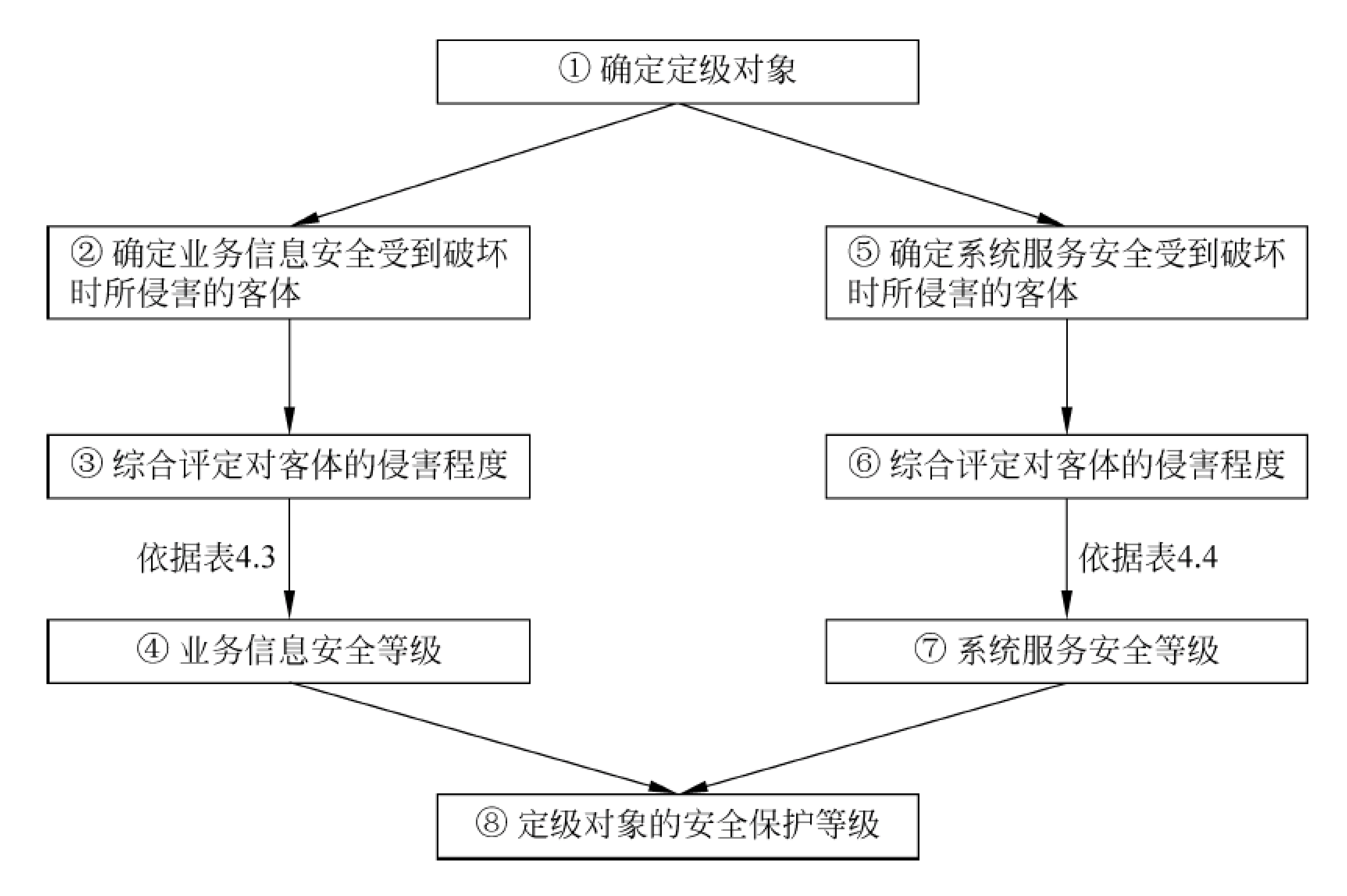


图 4.1　确定信息系统安全保护等级的一般流程

4. 等级确定

按上述流程的规定，在确定信息系统的安全保护等级(包括业务信息安全保护等级和系统服务安全保护等级)时需要准确地识别出被定级的信息系统受到破坏后，被侵害的客体以及这些客体被侵害的程度。这里所说的识别受侵害的客体和客体受侵害的程度都需要具体的可观察的指标，下面分别予以描述。

1) 确定待定级对象(信息系统)受到破坏而侵害的客体

依本节“2. 定级要素”中的定义，待定级对象(信息系统)受到破坏时所侵害的客体包括国家安全、社会秩序、公共利益，以及公民、法人和其他组织的合法权益。

为便于观察，将侵害国家安全的事项具体分解为以下所述的形式：

- 影响国家政权稳固和国防实力；
- 影响国家统一、民族团结和社会安定；
- 影响国家对外活动中的政治、经济利益；
- 影响国家重要的安全保卫工作；
- 影响国家经济竞争力和科技实力；
- 其他损害国家安全的事项。

将侵害社会秩序的事项分解为以下所述的形式：

- 影响国家机关社会管理和公共服务的工作秩序；
- 影响各种类型的经济活动秩序；
- 影响各行业的科研、生产秩序；
- 影响公众在法律约束和道德规范下的正常生活秩序等；
- 其他损害社会秩序的事项。

将影响公共利益的事项分解为以下所述的形式：

- 影响社会成员使用公共设施；
- 影响社会成员获取公开信息资源；
- 影响社会成员接受公共服务等；
- 其他影响公共利益的事项。

影响公民、法人和其他组织的合法权益是指由法律确认的、并受法律保护的公民、法人和其他组织所享有的社会权力和利益。

考察定级对象（信息系统）受到破坏后所侵害的客体时，应首先判断是否损害国家安全，然后判断是否损害社会秩序或公共利益，最后判断是否侵害公民、法人和其他组织的合法权益。这是确定保护等级由高到低的降序方法。

各行业可根据本行业的业务特点分析各类信息和各类信息系统与国家安全、社会秩序、公共利益，以及公民、法人和其他组织的合法权益的关系，从而确定本行业各类信息和各类信息系统受到破坏时所侵害的客体。

2）确定待定级对象（信息系统）受到破坏后对客体的侵害程度

对客体的侵害表现为对定级对象（信息系统）的破坏，其具体表现形式为对业务信息安全的破坏和对信息系统服务的破坏。其中，对业务信息安全的破坏是指破坏信息系统内信息的保密性、完整性和可用性等；对系统服务安全的破坏是指破坏信息系统可以及时、有效地提供服务，以完成预定的业务目标的功能和能力。由于业务信息安全和系统服务安全受到破坏时被侵害的客体所受的侵害程度可能会有所不同，因此在定级过程中需要分别对客体受侵害的程度予以考查。

业务信息安全和系统服务安全受到破坏后，下列危害后果是可以观测的：

- 降低或丧失服务职能；
- 业务能力下降；
- 引起法律纠纷；
- 导致财产损失；
- 造成不良社会影响；
- 对其他组织和个人造成损失；
- 其他影响。

这些表现形式可向上归类到受侵害的客体内，例如“造成不良社会影响”可以归类到侵害“社会秩序”这一客体，“导致财产损失”可以归类到侵害“公民、法人或其他组织的合法权益”这一客体，等等。

侵害程度是客观方面的不同外在表现的综合体现，因此，应首先根据不同的受侵害客体、不同的危害后果分别确定其危害程度。对不同危害后果确定其危害程度所采取的方法和所考虑的角度可能不同，例如系统服务安全被破坏导致业务能力下降的程度可以从信息系统服务覆盖的区域范围、用户人数或业务量等不同方面确定，业务信息安全被破坏导致的财物损失可以从直接的资金损失大小、间接的信息恢复费用等方面进行确定。

在判断不同的客体受侵害程度时应参照以下判别基准：

- 如果受侵害客体是公民、法人或其他组织的合法权益，则以本人或本单位的总体利益作为判断侵害程度的基准；
- 如果受侵害客体是社会秩序、公共利益或国家安全，则应以整个行业或国家的总体

利益作为判断侵害程度的基准；

- 如果受侵害客体是国家安全，则应在国家安全法的框架内以国家安全主管部门的指导意见作为判断侵害程度的基准。

对待定级对象（信息系统）受破坏后对客体的损害程度描述如下：

（1）一般损害。

受侵害客体具有下列情况之一：

- 工作职能受到局部影响，业务能力有所降低，但不影响主要功能的执行；
- 出现的法律纠纷不大；
- 财产损失较小；
- 对社会的不良影响较小；
- 对其他组织和个人造成的损害较低。

（2）严重损害。

受侵害客体具有下列情况之一：

- 工作职能受到严重影响，业务能力显著下降，且严重影响主要功能执行；
- 出现较严重的法律问题；
- 财产损失较大；
- 社会不良影响面较大；
- 对其他组织和个人造成的损害较严重。

（3）特别严重损害。

受侵害客体具有下列情况之一：

- 工作职能受到特别严重影响或丧失行使能力；
- 业务能力严重下降或功能无法执行；
- 出现极其严重的法律问题；
- 财产损失极大；
- 社会不良影响的范围广泛；
- 对其他组织和个人造成的损害非常严重。

利用上述观测指标进行判断时，可能在一种危害程度类型中具有不止一种情况，但只需要一种情况就可以作为判断的依据进行定级，例如在“严重损失”的描述中既有比较严重的法律问题，又存在影响面较大的社会影响，则根据一种情况即可定级；如在几种危害程度类型中都可以找到受害的情况，则以危害程度最高的作为定级的依据，例如既存在极严重的法律问题，又出现较大的财产损失，则应根据“极严重的法律问题”来确定保护等级。

业务信息安全和系统服务安全被破坏后对客体的侵害程度通过对受侵害的不同客体所遭受的危害程度进行综合评定得出。由于各行业信息系统所处理的信息种类和系统服务特点各不相同，业务信息安全和系统服务安全受到破坏后客体所受侵害程度的计算方式均可能不同，各行业可根据本行业的业务信息特点和系统服务特点在上述方法的指导下制定符合本单位实际的危害程度的综合评定体系，并给出侵害不同客体造成一般损害、严重损害、特别严重损害的具体定义。

根据业务信息安全被破坏时所侵害的客体以及对相应客体的侵害程度，依据表 4.3 所示的业务信息安全保护等级矩阵表即可得到业务信息安全保护等级。

表 4.3　业务信息安全保护等级矩阵表

业务信息安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

根据系统服务安全被破坏时所侵害的客体以及对相应客体的侵害程度，依据表 4.4 所示的系统服务安全保护等级矩阵表即可得到系统服务安全保护等级。

表 4.4　系统服务安全保护等级矩阵表

系统服务安全被破坏时所侵害的客体	对相应客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

作为定级对象的信息系统的安全保护等级由业务信息安全保护等级和系统服务安全保护等级的较高者决定。

信息系统运营、使用单位依据《信息系统安全等级保护定级指南》确定信息系统的安全保护等级后，有主管部门的，应将确定的信息系统安全保护等级报请主管部门审核批准。

同一行业、业务系统跨省运行的或者全国统一联网运行的信息系统可以由主管部门统一确定安全保护等级。

对拟确定为第四级(含)以上信息系统的，运营、使用单位或者主管部门应当邀请具有资质的信息安全保护等级专家组成评审委员会进行评审。

4.2.2　安全等级保护工作的监管

信息系统运营、使用单位依据管理办法和相关技术标准对信息系统进行保护，国家有关信息安全监管部门对其信息安全等级保护工作进行监督管理。这里所说的运营单位指负责电子政务信息系统、重要信息系统、企事业信息系统运营的单位，可以是这些信息系统的所有者或管理者单位，也可以是受特别委托的国家授权的第三方组织；使用单位则是利用信息系统完成或执行工作职能的组织或机构。

实行第一级安全保护的信息系统运营、使用单位依据国家有关管理规范和技术标准自主进行保护。

实行第二级安全保护的信息系统运营、使用单位除依据国家有关管理规范和技术标准自主进行保护外，还需接受国家信息安全监管部门对该级信息系统信息安全等级保护工作的指导。

实行第三级安全保护的信息系统运营、使用单位在依据国家有关管理规范和技术标准进行保护的过程中必须接受国家信息安全监管部门对该级信息系统信息安全等级保护工作的监督、检查。

实行第四级安全保护的信息系统运营、使用单位在依据国家有关管理规范、技术标准和业务专门需求进行保护的过程中，国家信息安全监管部门对该级信息系统信息安全等级保护工作进行强制监督、检查。

实行第五级安全保护的信息系统运营、使用单位在依据国家有关管理规范、技术标准和业务特殊安全需求进行保护的过程中，由国家信息安全监管机构指定专门部门对该级信息系统信息安全等级保护工作进行专门监督、检查。

4.2.3 安全等级保护的实施

信息系统的安全保护等级确定后，运营、使用单位应当按照国家信息安全等级保护管理规范和技术标准，使用符合国家有关规定，满足信息系统安全保护等级需求的信息技术产品，开展信息系统安全建设或者改建工作。

信息系统运营、使用单位应按照《信息系统安全等级保护实施指南》实施等级保护工作。

在信息系统建设过程中，运营、使用单位应当按照《信息系统安全等级保护基本要求》等技术标准，参照《信息安全技术　信息系统通用安全技术要求》(GB/T 20271—2006)、《信息安全技术　网络基础安全技术要求》(GB/T 20270—2006)、《信息安全技术　操作系统安全技术要求》(GB/T 20272—2006)、《信息安全技术　数据库管理系统安全技术要求》(GB/T 20273—2006)、《信息安全技术　服务器技术要求》、《信息安全技术　终端计算机系统安全等级技术要求》(GA/T 671—2006)等技术标准同步建设符合该等级要求的信息安全设施。

4.2.3.1 基本原则

信息系统安全等级保护管理的核心是对信息系统划分保护等级、按相关标准进行建设、管理和监督。信息系统安全等级保护在实施过程中应遵循以下基本原则：

1. 自主保护与监管相结合

信息系统运营、使用单位及其主管部门遵循国家相关法规和标准，依照确定的信息系统的安全保护等级自行组织实施安全保护。在实施安全保护的过程中，需要由国家信息安全监管部门指导的(第二级安全保护等级)，应主动征询指导意见；需要接受国家信息安全监管部门监督、检查(第三级安全保护等级)或强制监督、检查的(第四级安全保护等级)，应自觉接受监督、检查；需要由国家安全监管机构指定专门部门进行专门监督、检查的(第五级安全保护等级)，应主动予以配合。

2. 重点保护

根据信息系统的重要程度、业务特点划分不同的安全保护等级，实现不同强度的安全保护，从而集中安全资源优先保护涉及核心业务或关键信息的资产。

3. 同步建设

信息系统在新建、改建、扩建时应当同步规划和设计安全方案，投入一定比例的资金建设、变更、健全信息安全设施，确保信息安全与信息化建设相适应。

4. 动态调整

我们要跟踪信息系统的变化情况，随之调整安全保护措施。由于信息系统的应用类型、应用范围或服务能力以及使用环境等条件发生变化，安全保护等级需要进行变更的，应当根据等级保护的管理规范和技术标准的要求重新确定信息系统的安全保护等级，根据信息系统安全保护等级的变化情况调整安全保护方案并重新实施安全保护。

4.2.3.2 角色和职责

信息系统安全等级保护实施过程中涉及各种角色，它们各自有不同的职责，共同维护我国各类信息系统的安全等级保护。

1. 国家管理部门

公安机关负责信息系统安全等级保护工作的监督、检查、指导；国家保密工作部门负责国家秘密信息系统安全等级保护工作中的监督、检查、指导；国家密码管理部门负责各类信息系统安全等级保护工作中有关密码工作的监督、检查、指导；涉及其他职能部门管辖范围的事项由有关职能部门依照国家法律法规的规定进行管理；国务院信息化工作办公室及地方信息化领导小组办事机构负责等级保护工作的部门间协调。

2. 信息系统主管部门

国家机关或政府部门负责依照国家信息安全等级保护的管理规范和技术标准督促、检查和指导本行业、本部门或者本地区信息系统运营、使用单位的信息安全等级保护工作。

3. 信息系统运营、使用单位

信息系统运营、使用单位负责依照国家信息安全等级保护的管理规范和技术标准确定其信息系统的安全保护等级，有主管部门的，应当报其主管部门审核批准；根据已经确定的安全保护等级到公安机关办理备案手续(涉密信息系统除外)；按照国家信息安全等级保护管理规范和技术标准进行信息系统安全等级保护的规划、设计；使用符合国家有关规定满足信息系统安全保护等级需求的信息技术产品和信息安全产品开展信息系统安全建设或者改建工作；制定、落实各项安全管理制度，定期对信息系统的安全状况、安全保护制度及措施的落实情况进行自查，选择符合国家相关规定的安全保护等级测评机构，定期进行安全保护等级的测评；制定不同等级信息安全事件的响应、处置预案，对信息系统的信息安全事件分等级进行应急处置。

4. 信息安全服务机构

获得国家主管机关批准的具有资质和能力的信息安全服务从业法人单位接受信息系统运营、使用单位的委托，依照国家信息安全等级保护的管理规范和技术标准为信息系统运营、使用单位完成等级保护的相关工作提供咨询或协助服务，包括参与确定其信息系统的安全保护等级、进行安全需求分析、安全措施总体规划、实施安全建设和安全改造等。

5. 信息安全等级测评机构

由国家授权成立的特殊的信息安全服务机构受信息系统运营、使用单位的委托或根据国家管理部门的委托，协助信息系统运营、使用单位或国家管理部门按照国家信息安全等级保护的管理规范和技术标准对已经完成等级保护建设的信息系统进行安全等级测评；对信息安全产品供应商提供的信息安全产品进行安全等级保证的有效性测评。

6. 信息安全产品供应商

获得国家主管机构批准的信息安全产品的生产和销售的法人单位按照国家信息安全等级保护的管理规范和技术标准开发符合等级保护相关要求的信息安全产品，接受安全等级测评机构的检测；按照等级保护相关要求销售信息安全产品并提供售后服务。

4.2.3.3 实施流程

实施信息系统安全等级保护的基本流程如图4.2所示。

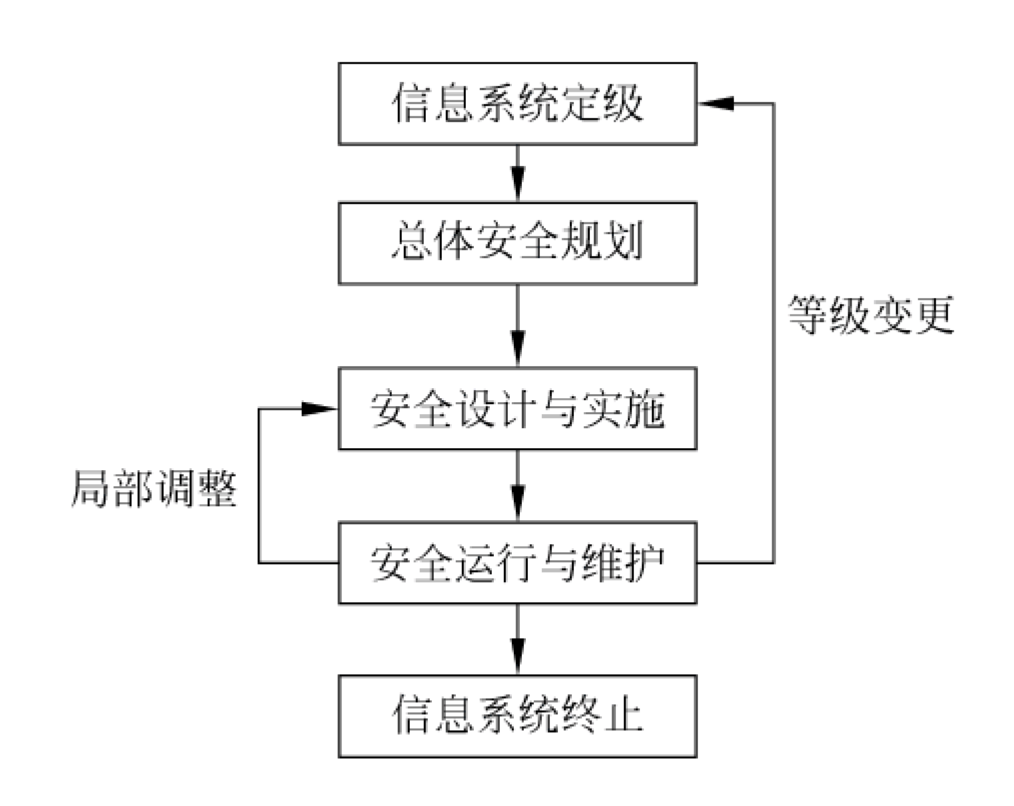


图 4.2　信息系统安全等级保护实施的基本流程

在安全运行与维护阶段，信息系统因需求变化等原因导致局部调整，但信息系统的安全保护等级并未改变，此时应从安全运行与维护阶段返回到安全设计与实施阶段，对已设计的安全措施进行调整然后予以实施，确保满足信息系统局部调整后的安全等级保护的要求；如信息系统发生重大变更导致其安全保护等级变化时，应从安全运行与维护阶段返回到信息系统定级阶段，开始新一轮信息安全等级保护的实施过程。

1. 信息系统定级

信息系统定级阶段的目标是信息系统运营、使用单位按照国家有关管理规范和《信息系统安全等级保护指南》确定信息系统的安全保护等级，并按规定报有关部门备案或审核批准。

1）实施信息系统定级

信息系统定级阶段的工作流程如图 4.3 所示。

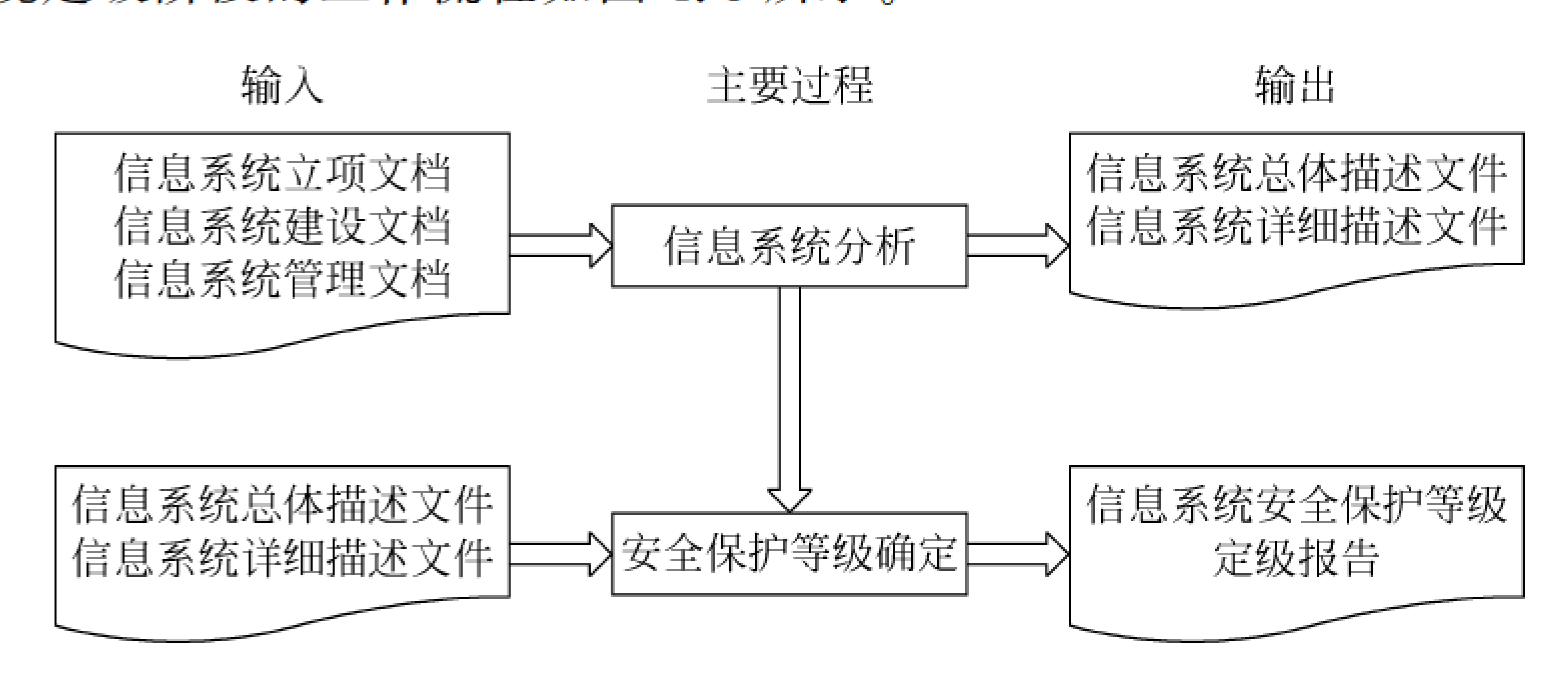


图 4.3　信息系统定级阶段的工作流程

需要注意的是，这一阶段的工作流程与图 4.1（确定信息系统安全保护等级的一般流程）不是一回事，前者（图 4.3）说明具体的定级实务操作，后者（图 4.1）说明定级阶段中在“安全保护等级确定”这一步骤中使用的方法，两者不可混淆。

2）信息系统分析

（1）系统识别和描述

① 活动目标：本阶段活动的目标是通过从信息系统运营、使用单位相关人员处收集有关信息系统的信息，并对收集的信息进行整理和综合分析，依据整理和分析的内容形成组织

机构内信息系统的总体描述性文档。

② 参与角色：信息系统运营、使用单位，信息安全服务机构。

③ 活动输入：信息系统的立项、建设和管理文档。

④ 活动描述：本活动主要包括以下子项内容。

- 识别信息系统的基本信息：调查了解信息系统的行业特征、主管机构、业务范围、地理位置以及信息系统构成的基本情况，获得信息系统的背景信息。
- 识别信息系统的管理框架：了解信息系统所在组织的管理结构、管理策略、部门设置和部门在业务运行中的作用、岗位职责，获得支持信息系统业务运营的管理特征和管理框架方面的信息，从而明确信息系统的安全责任主体。
- 识别信息系统的网络及设备部署：了解信息系统的物理环境、网络拓扑结构和硬件设备的部署情况，在此基础上明确信息系统的边界，即确定定级对象及其范围。
- 识别信息系统的业务种类和特性：了解机构内主要依靠信息系统处理的业务的种类和数量，以及这些业务各自的社会属性、业务内容和业务流程等，明确支持机构业务运营的信息系统的业务特性，将承载比较单一的业务应用或者承载相对独立的业务应用的信息系统作为单独的定级对象。
- 识别业务系统处理的信息资产：了解业务系统处理的信息资产的类型，以及这些信息资产在保密性、完整性和可用性等方面的重要程度。
- 识别用户范围和用户类型：根据用户或用户群的分布范围了解业务系统的服务范围、作用以及业务连续性方面的要求等。
- 信息系统描述：对收集的信息进行整理、分析，形成对信息系统的总体描述文件。一个典型的信息系统的总体描述文件应包含以下内容。
  - 系统概述；
  - 系统边界描述；
  - 网络拓扑；
  - 设备部署；
  - 支撑的业务应用的种类和特性；
  - 处理的信息；
  - 用户的范围和用户类型；
  - 信息系统的管理框架。

活动输出：信息系统总体描述文件。

(2) 信息系统的划分

① 活动目标：本阶段活动的目标是依据信息系统的总体描述文件在综合分析的基础上将组织机构内运行的信息系统进行合理分解，确定所包含的可以作为定级对象的信息系统的个数。

② 参与角色：信息系统运营、使用单位，信息安全服务机构。

③ 活动输入：信息系统总体描述文件。

④ 活动描述：本活动主要包括以下子项内容。

- 子系统划分方法的选择：一个组织机构可能运行一个大型信息系统，为了突出重点保护的等级保护原则，应对大型信息系统进行划分，进行信息系统划分的方法有多

种，可以考虑管理机构、业务类型、物理位置等因素，信息系统的运营、使用单位应该根据本单位的具体情况确定系统的划分原则。

- 信息子系统的划分：依据选择的子系统划分原则，将一个组织机构内拥有的大型信息系统进行划分，划分出相对独立的信息子系统并作为定级对象，应保证每个相对独立的信息子系统具备定级对象的基本特征。在划分信息系统的过程中，应该首先考虑组织管理的要素，然后考虑业务类型、物理区域等要素。
- 信息系统的详细描述：在对信息系统进行划分并确定定级对象后，应在信息系统总体描述文件的基础上进一步增加信息系统划分信息的描述，准确地描述一个大型信息系统中包括的定级对象的个数。

进一步的信息系统详细描述文件应包含以下内容：

- 相对独立的信息子系统列表；
- 每个定级对象(大型信息系统中相对独立的信息子系统，下同)的概述；
- 每个定级对象的边界；
- 每个定级对象的设备部署；
- 每个定级对象支撑的业务应用及其处理的信息资产类型；
- 每个定级对象的服务范围和用户类型；
- 其他应该描述的内容。

活动输出：信息系统详细描述文件。

3）安全保护等级确定

(1) 定级、审核和批准

① 活动目标：本阶段活动的目标是按照国家有关管理规范和《信息安全等级保护的定级指南》(GB/T 22240—2008)确定信息系统的安全保护等级，并对定级结果进行审核和批准，保证定级结果的准确性和合法性。

② 参与角色：信息系统主管部门，信息系统运营、使用单位，信息安全服务机构。

③ 活动输入：信息系统总体描述文件、信息系统详细描述文件。

④ 活动描述：本活动主要包括以下子项内容。

- 初步确定信息系统安全保护等级：根据国家有关管理规范和《信息安全等级保护的定级指南》(GB/T 22240—2008)确定的定级方法，信息系统运营、使用单位对每个定级对象确定初步的安全保护等级。
- 定级结果审核和批准：信息系统运营、使用单位初步确定了安全保护等级后，有主管部门的，应当经主管部门审核批准；跨省或者全国统一联网运行的信息系统可以由主管部门统一确定安全保护等级；对拟确定为第四级以上信息系统的，运营使用单位或者主管部门应当邀请国家信息安全保护等级专家评审委员会评审。

活动输出：信息系统定级评审意见。

(2) 形成定级报告

① 活动目标：本阶段活动的目标是对定级过程中产生的文档进行整理，形成信息系统定级结果报告。

② 参与角色：信息系统主管部门，信息系统运营、使用单位。

③ 活动输入：信息系统总体描述文件、信息系统详细描述文件、信息系统定级结果。

④ 活动描述：对信息系统的总体描述文档、信息系统的详细描述文件、信息系统安全保护等级定级结果等内容进行整理，形成文件化的信息系统定级结果报告。

信息系统定级结果报告可以包含以下内容：

- 单位信息化现状概述；
- 管理模式；
- 定级对象(信息系统)列表；
- 每个信息系统的概述；
- 每个信息系统的边界；
- 每个信息系统的设备部署；
- 每个信息系统支撑的业务应用；
- 信息系统列表、安全保护等级以及保护要求的组合；
- 其他应该描述的内容。

2. 总体安全规划

1) 总体安全规划阶段的工作流程

总体安全规划阶段的目标是根据信息系统的划分情况、信息系统的定级情况、信息系统承载的业务情况，通过分析明确信息系统安全需求，设计合理的、满足等级保护要求的总体安全方案，并制定出安全实施计划，以指导后续的信息系统安全建设工程实施。对于已运营(运行)的信息系统，安全需求分析应当首先分析判断信息系统的安全保护现状与等级保护要求之间的差距。

总体安全规划阶段的工作流程见图 4.4。

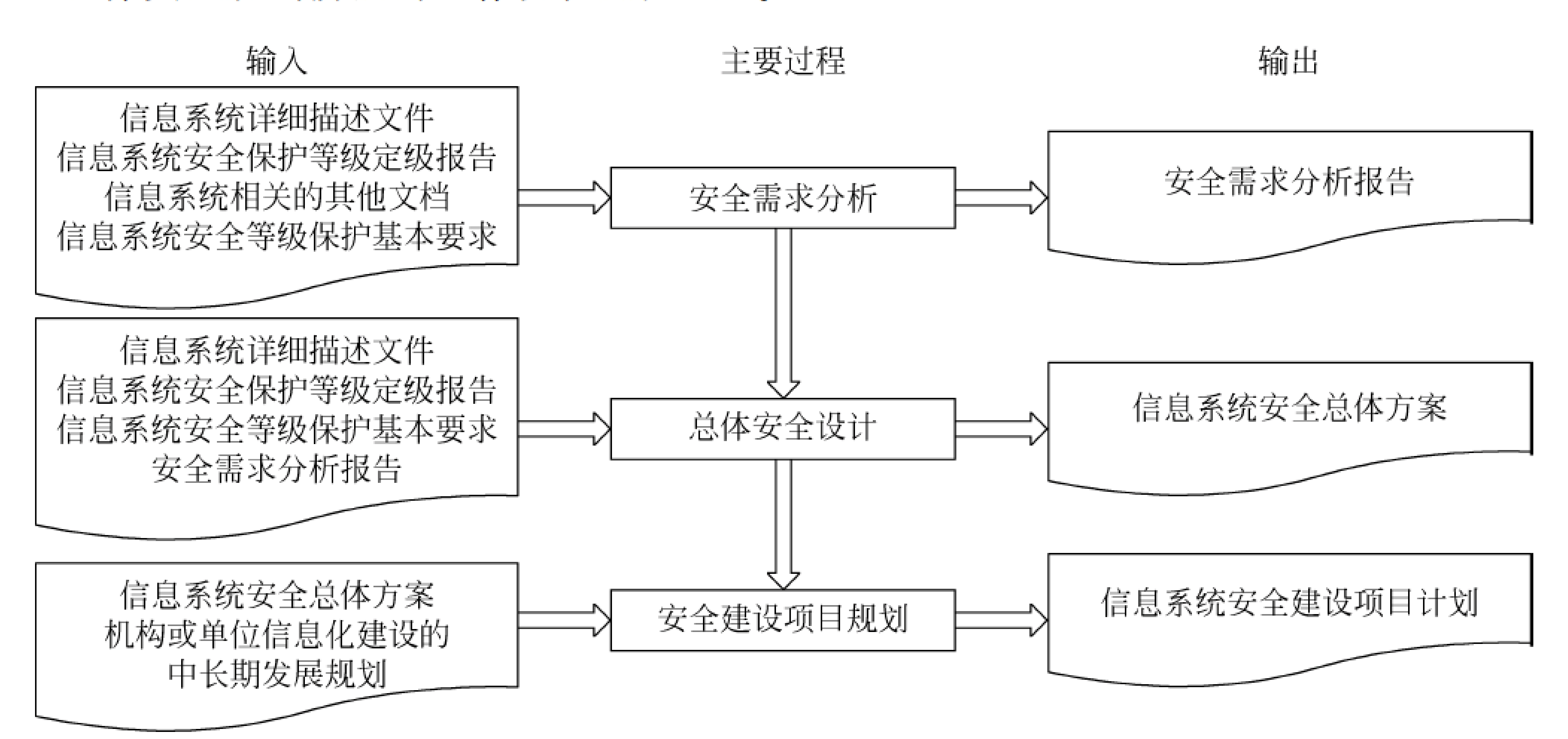


图 4.4　总体安全规划阶段的工作流程

2) 安全需求分析

(1) 基本安全需求的确定

① 活动目标：本阶段活动的目标是根据信息系统的安全保护等级判断信息系统现有的安全保护水平与国家等级保护管理规范和技术标准之间的差距，提出信息系统的基本安全保护需求。

② 参与角色：信息系统运营、使用单位，信息安全服务机构，信息安全等级测评机构。

③ 活动输入：信息系统详细描述文件、信息系统安全保护等级定级报告、信息系统相关的其他文档、信息系统安全等级保护基本要求。

④ 活动描述：本活动主要包括以下子项内容。

- 确定系统范围和分析对象：明确不同安全保护等级信息系统的范围和边界，通过调查或查阅资料的方式了解信息系统的构成，包括网络拓扑、业务应用、业务流程、设备信息、安全措施状况等，初步确定每个需要保护的信息系统内的分析对象，包括整体对象，例如机房、办公环境、网络等，也包括具体对象，例如边界设备、网关设备、服务器设备、工作站、应用系统等。
- 形成评价指标和评估方案：根据对各个信息系统已确定的安全保护等级从信息系统安全保护等级评价指标体系(即根据本单位业务信息特点和系统服务特点对业务信息和系统服务受破坏的客体以及客体受危害的程度设计出的与相应安全保护等级具有对应性的具体评价指标的一个集合)中选择相应等级的评价指标，根据评价指标结合确定的具体对象制定可以操作的评估方案，评估方案可以包含以下内容。

管理状况评估表；

网络状况评估表；

网络设备(含安全设备)评估表；

主机设备评估表；

主要设备安全测试方案；

重要操作的作业指导书。

- 现状与评价指标对比：通过考察现场、询问人员、查询资料、检查记录、检查配置、技术测试、渗透攻击等方式进行安全技术和安全管理方面的评估，判断安全技术和安全管理的各个方面与评价指标的符合程度，给出判断结论，依此确定信息系统安全保护的基本需求。

活动输出：基本安全需求。

(2) 额外/特殊安全需求的确定

① 活动目标：本阶段活动的目标是通过对信息系统重要资产特殊保护要求的分析确定超出相应等级保护基本要求的部分或具有特殊安全保护要求的部分，采用需求分析和残留风险分析相结合的方法确定可能存在的安全风险，判断对超出等级保护基本要求部分实施特殊安全措施的必要性，提出信息系统的特殊安全保护需求。

② 参与角色：信息系统运营、使用单位，信息安全服务机构。

③ 活动输入：信息系统详细描述文件、信息系统安全保护等级定级报告、信息系统相关的其他文档。

④ 活动描述：确定特殊安全需求可以采用目前成熟或流行的需求分析和残留风险分析方法，或者采用下面的步骤。

- 确定重要资产的分布：明确信息系统的重要或关键部件，例如边界设备、网关设备、核心网络设备、重要服务器设备、重要应用系统等。
- 评估重要资产的安全弱点：检查或判断上述重要部件可能存在的脆弱点，包括技术上和管理上的脆弱点；分析安全脆弱点被利用的可能性。

- 评估重要资产面临的威胁：分析和判断上述重要部件的脆弱性可能面临的威胁，包括来自外部的威胁和来自内部的威胁，研判威胁发生的可能性或概率。
- 综合风险分析：分析威胁利用脆弱点可能产生的结果，结果造成的损害或影响的大小，以及避免上述结果产生的可能性、必要性和经济性，按照重要资产的排序和风险的排序确定特殊安全保护的要求。

活动输出：重要资产的特殊保护要求。

(3) 形成安全需求分析报告

① 活动目标：本阶段活动的目标是总结基本安全需求和特殊安全需求，形成安全需求分析报告。

② 参与角色：信息系统运营、使用单位，信息安全服务机构。

③ 活动输入：信息系统详细描述文件、信息系统安全保护等级定级报告、基本安全需求、重要资产的特殊保护要求。

④ 活动描述：本活动主要包括以下内容。

完成安全需求分析报告，即根据基本安全需求和特殊的安全保护需求等形成安全需求分析报告。安全需求分析报告可以包含以下内容：

信息系统描述；

安全管理状况；

安全技术状况；

存在的不足和可能的风险；

安全需求描述。

活动输出：安全需求分析报告。

3) 总体安全设计

(1) 总体安全战略设计

① 活动目标：本阶段活动的目标是形成组织机构纲领性的信息安全战略文件，包括确定安全目标和安全方针，制定安全策略，以便结合等级保护基本要求和安全保护特殊要求构建组织机构信息系统的安全技术体系结构和安全管理体系结构。

② 参与角色：信息系统运营、使用单位，信息安全服务机构。

③ 活动输入：信息系统详细描述文件、信息系统安全保护等级定级报告、安全需求分析报告。

④ 活动描述：本活动主要包括以下子活动内容。

- 确定信息安全的总体目标。
- 确定安全方针：形成组织机构最高层次的安全方针文件，阐明安全工作的使命和意志，规定信息安全责任机构和职责，建立安全工作运行模式等。
- 制定安全策略：形成机构高层次的安全策略文件，说明安全工作的主要策略，包括安全组织机构划分策略、业务系统分级策略、数据信息分级策略、子系统互连策略、信息流控制策略等。

活动输出：总体安全战略文件。

(2) 安全技术体系结构设计

① 活动目标：本阶段活动的目标是根据信息系统安全等级保护基本要求、安全需求分

析报告、机构总体安全战略文件等提出系统需要实现的安全技术措施，形成机构特定的系统安全技术体系结构，用于指导信息系统分等级保护的具体实现。

② 参与角色：信息系统运营、使用单位，信息安全服务机构。

③ 活动输入：信息系统详细描述文件、信息系统安全保护等级定级报告、安全需求分析报告、机构总体安全战略文件、信息系统安全等级保护基本要求。

④ 活动描述：本活动主要包括以下子项内容。

- 规定骨干网/城域网的安全保护技术措施：根据机构总体安全战略文件、等级保护基本要求和安全需求提出骨干网/城域网的安全保护策略和安全技术措施。在提出骨干网/城域网的安全保护策略和安全技术措施时应考虑网络线路和网络设备共享的情况，如果不同级别的子系统通过骨干网/城域网的同一线路和设备传输数据，线路和设备的安全保护策略和安全技术措施应满足最高级别子系统的等级保护基本要求。
- 规定子系统之间互联的安全技术保护措施：根据机构总体安全战略文件、等级保护基本要求和安全需求，提出跨局域网互联的子系统之间的信息传输保护策略要求和具体的安全技术保护措施，包括同级互联的策略、不同级别互联的策略等；提出局域网内部互联的子系统之间的信息传输保护策略要求和具体的安全技术保护措施，包括同级互联的策略、不同级别互联的策略等。
- 规定不同级别子系统的边界保护技术措施：根据机构总体安全战略文件、等级保护基本要求和安全需求提出不同级别子系统边界的安全保护策略和安全技术措施。在提出子系统边界安全保护策略和安全技术措施时应考虑边界设备共享的情况，如果不同级别的子系统通过同一设备进行边界保护，这个边界设备的安全保护策略和安全技术保护措施应满足最高级别子系统的等级保护基本要求。
- 规定不同级别子系统内部系统平台和业务应用的安全保护技术措施：根据机构总体安全战略文件、等级保护基本要求和安全需求提出不同级别子系统内部网络平台、系统平台和业务应用的安全保护策略和安全技术保护措施。
- 规定不同级别信息系统机房的安全保护技术措施：根据机构总体安全战略文件、等级保护基本要求和安全需求提出不同级别信息系统机房的安全保护策略和安全技术保护措施。在提出信息系统机房安全保护策略和安全技术保护措施时，应考虑不同级别的信息系统共享机房的情况，如果不同级别的信息系统共享同一机房，机房的安全保护策略和安全技术措施应满足最高级别信息系统的等级保护基本要求。
- 形成信息系统安全技术体系结构：将骨干网/城域网、通过骨干网/城域网的子系统互联、局域网内部的子系统互联、子系统的边界、子系统内部各类平台、机房以及其他方面的安全保护策略和安全技术措施进行整理、汇总，形成信息系统的安全技术体系结构。

活动输出：形成描述信息系统安全技术体系结构的文档。

(3) 整体安全管理体系结构设计

① 活动目标：本阶段活动的目标是根据等级保护基本要求、安全需求分析报告、机构总体安全战略文件等调整原有管理模式和管理策略，既从全局高度考虑为每个等级信息系

统制定统一的安全管理策略，又从每个信息系统的实际需求出发，选择和调整具体的安全管理措施，最后形成统一的整体安全管理体系结构。

② 参与角色：信息系统运营、使用单位，信息安全服务机构。

③ 活动输入：信息系统详细描述文件、信息系统安全保护等级定级报告、安全需求分析报告、机构总体安全战略文件、信息系统安全等级保护基本要求。

④ 活动描述：本活动主要包括以下子项内容。

- 规定信息安全的组织管理体系和对各信息系统的安全管理职责：根据机构总体安全战略文件、等级保护基本要求和安全需求提出机构的安全组织管理机构框架，分配各等级信息系统的安全管理职责，制定各等级信息系统的安全管理策略等。
- 制定各保护等级信息系统的人员安全管理策略：根据机构总体安全战略文件、等级保护基本要求和安全需求提出各等级信息系统的管理人员框架，分配各等级信息系统的管理人员职责，制定各等级信息系统的人员安全管理策略等。
- 制定各等级信息系统机房及办公区等物理环境的安全管理策略：根据机构总体安全战略文件、等级保护基本要求和安全需求提出各等级信息系统的机房和办公环境的安全策略。
- 制定各等级信息系统介质、设备等的安全管理策略：根据机构总体安全战略文件、等级保护基本要求和安全需求提出各等级信息系统的介质、设备等的安全策略。
- 制定各等级信息系统运行安全管理策略：根据机构总体安全战略文件、等级保护基本要求和安全需求提出各等级信息系统的安全运行与维护框架和运维安全策略等。
- 制定各等级信息系统安全事件处置和应急管理策略：根据机构总体安全战略文件、等级保护基本要求和安全需求提出各等级信息系统的安全事件处置和应急管理策略等。
- 形成信息系统安全管理策略框架：将上述各个方面的安全管理策略进行整理、汇总，形成信息系统的整体安全管理体系结构。

活动输出：形成描述信息系统安全管理体系结构的文档。

（4）设计结果文档化

① 活动目标：本阶段活动的目标是将总体安全设计工作的结果文档化，最后形成一套指导机构信息安全工作的指导性文件。

② 参与角色：信息系统运营、使用单位，信息安全服务机构。

③ 活动输入：安全需求分析报告、信息系统安全技术体系结构、信息系统安全管理体系结构。

④ 活动描述：对安全需求分析报告、信息系统安全技术体系结构和安全管理体系结构等文档进行整理，形成信息系统总体安全方案。

信息系统总体安全方案包含以下内容：

- 信息系统概述；
- 总体安全战略；
- 信息系统安全技术体系结构；
- 信息系统安全管理体系结构。

活动输出：信息系统安全总体方案。

4）安全建设项目规划

（1）安全建设目标的确定

① 活动目标：本阶段活动的目标是依据信息系统安全总体方案（由一个或多个文件构成）、机构或单位信息化建设的中长期发展规划和机构的安全建设资金状况确定各阶段的安全建设目标。

② 参与角色：信息系统运营、使用单位，信息安全服务机构。

③ 活动输入：信息系统安全总体方案、机构或单位信息化建设的中长期发展规划。

④ 活动描述：本阶段活动主要包括以下子项内容。

- 信息化建设中长期发展规划和安全需求调查：了解和调查单位信息化建设的现况、中长期信息化建设的目标、主管部门对信息化的资源投入，对比信息化建设过程中阶段状态与安全战略规划之间的差距，分析急迫和关键的安全问题，考虑可以同步进行的安全建设内容等。
- 提出信息系统安全建设分阶段目标：制定系统在规划期内（一般安全规划期为 3 年）所要实现的总体安全目标；制定系统短期（1 年以内）要实现的安全目标，主要解决目前急迫和关键的问题，争取在短期内安全状况有大幅度提高。

活动输出：信息系统分阶段安全建设目标。

（2）安全建设内容规划

活动目标：本阶段活动的目标是根据安全建设目标和信息系统安全总体方案的要求设计分期分批的主要建设内容，并将建设内容组合成不同的项目，阐明项目之间的依赖或促进关系等。

参与角色：信息系统运营、使用单位，信息安全服务机构。

活动输入：信息系统安全总体方案、信息系统分阶段安全建设目标。

活动描述：本活动主要包括以下子项内容。

- 确定主要安全建设内容：根据信息系统安全总体方案明确主要的安全建设内容，并将其进行适当的分解。其主要的安全建设内容可以分解为（但不限于）以下内容：
  - 安全基础设施建设；
  - 网络安全建设；
  - 系统平台和应用平台安全建设；
  - 数据系统安全建设；
  - 安全标准体系建设；
  - 人才培养体系建设；
  - 安全管理体系建设。
- 确定主要安全建设项目：将安全建设内容转化为不同的安全建设项目，描述项目所要解决的主要安全问题及所要达到的安全目标，对项目进行支持或依赖等关联性分析，对项目进行紧迫性分析，对项目进行实施难易程度分析，对项目进行预期效果（包括实施风险）分析，描述项目的具体工作内容、建设方案，形成安全建设项目列表。

活动输出：安全建设项目列表（含安全建设内容）。

（3）形成安全建设项目计划

活动目标：本阶段活动的目标是根据建设目标和建设内容在时间和经费上对安全建设

项目列表进行总体考虑，分配到不同的时期和阶段，设计建设顺序，进行投资估算，形成安全建设项目计划。

参与角色：信息系统运营、使用单位，信息安全服务机构。

活动输入：信息系统安全总体方案、信息系统分阶段安全建设目标、安全建设内容等。

活动描述：对信息系统分阶段安全建设目标、安全总体方案和安全建设内容等文档进行整理，形成信息系统安全建设项目计划。

安全建设项目计划可包含以下内容：

- 规划建设的依据和原则；
- 规划建设的目标和范围；
- 信息系统安全现状；
- 信息化的中长期发展规划；
- 信息系统安全建设的总体框架；
- 安全技术体系建设规划；
- 安全管理与安全保障体系建设规划；
- 安全建设投资估算；
- 信息系统安全建设的实施保障等内容。

活动输出：信息系统安全建设项目计划。

3. 安全设计与实施

1）安全设计与实施阶段的工作流程

安全设计与实施阶段的目标是按照信息系统安全总体方案的要求结合信息系统安全建设项目计划分期分步落实安全措施。

安全设计与实施阶段的工作流程见图 4.5。

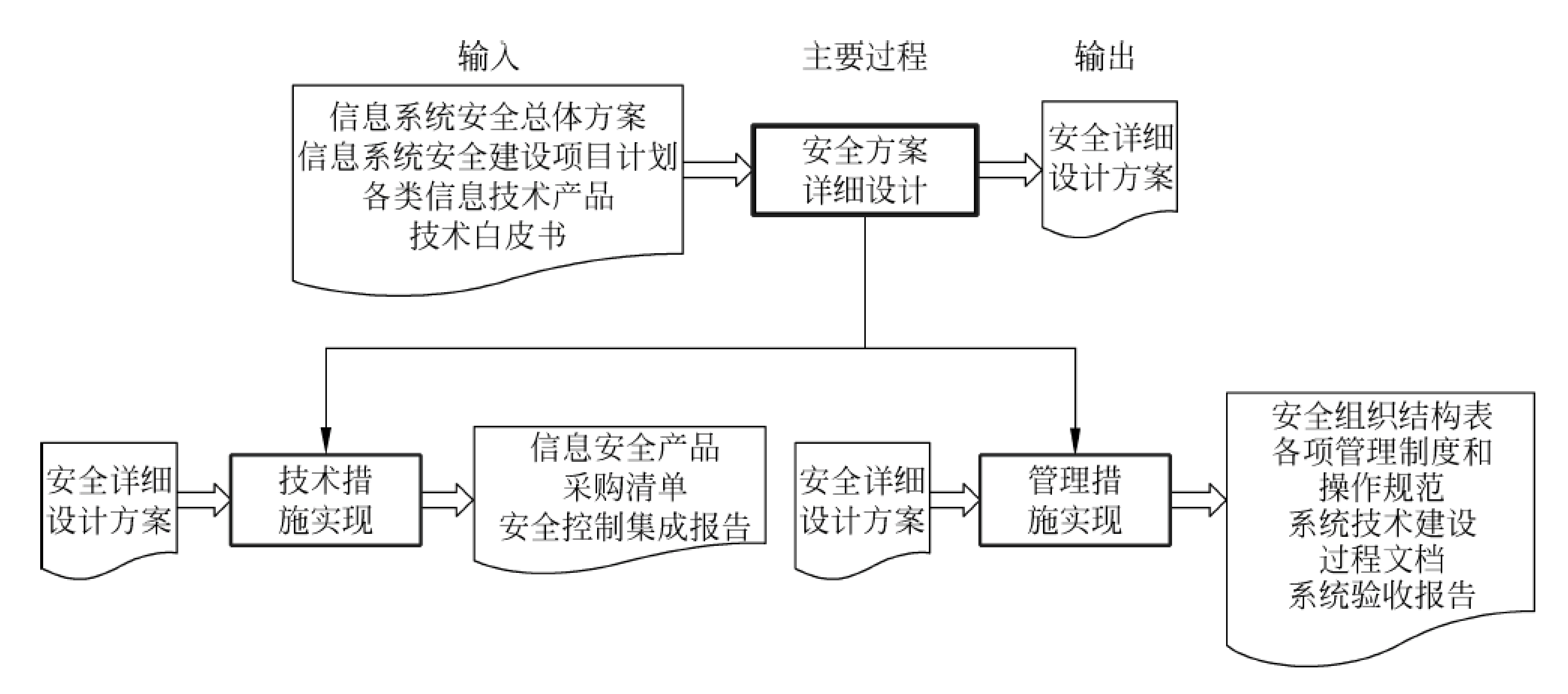


图 4.5　安全设计与实施流程图

2）安全方案详细设计

（1）技术措施实现内容设计

活动目标：本阶段活动的目标是根据建设目标和建设内容将信息系统安全总体方案中要求实现的安全策略、安全技术体系结构、安全措施和要求落实到产品功能或物理形态上，

提出能够实现的产品或组件及其具体规范，并将产品功能特征整理成文档，使得在信息安全产品采购和安全控制开发阶段有据可依。

参与角色：信息系统运营、使用单位，信息安全服务机构，信息安全产品供应商。

活动输入：信息系统安全总体方案、信息系统安全建设项目计划、各类信息技术产品和信息安全产品技术白皮书。

活动描述：本活动主要包括以下子项内容。

- 结构框架设计：依据本次实施项目的建设内容和信息系统的实际情况给出与总体安全规划阶段的安全体系结构一致的安全实现技术框架，内容可能包括安全防护的层次、信息安全产品的使用、网络子系统的划分、IP 地址的规划等内容。
- 功能/性能要求设计：对安全实现技术框架中使用到的相关信息安全产品，例如防火墙、VPN、网闸、认证网关、代理服务器、网络防病毒、PKI 等提出功能/性能指标要求，对需要开发的安全控制组件提出功能/性能指标要求。
- 部署方案设计：结合目前信息系统网络拓扑以图示的方式给出安全技术实现框架的实现方式，包括信息安全产品或安全组件的部署位置、连接方式、IP 地址分配等，对于需对原有网络进行调整的，给出网络调整的图示方案等。
- 制定安全策略实现计划：依据信息系统安全总体方案中提出的安全策略的要求制定设计和设置信息安全产品或安全组件的安全策略实现计划。

活动输出：技术措施落实方案。

(2) 管理措施实现内容设计

活动目标：本阶段活动的目标是根据机构当前安全管理需要和安全技术保障需要提出与信息系统安全总体方案中管理部分相适应的本期安全管理的实施内容，以保证在安全技术保护措施建设的同时同步实现安全管理措施。

参与角色：信息系统运营、使用单位，信息安全服务机构。

活动输入：信息系统安全总体方案、信息系统安全建设项目计划。

活动描述：结合系统实际安全管理需要和本次技术建设内容确定本次安全管理建设的范围和内容，同时注意与信息系统安全总体方案的一致性。安全管理设计的内容主要考虑安全管理机构和人员的配套、安全管理制度的配套、人员安全管理技能的配套等。

活动输出：管理措施落实方案。

(3) 设计结果文档化

活动目标：本阶段活动的目标是将技术措施落实方案、管理措施落实方案汇总，同时考虑工时和费用，最后形成指导安全实施的指导性文件。

参与角色：信息系统运营、使用单位，信息安全服务机构。

活动输入：技术措施落实方案、管理措施落实方案。

活动描述：对技术措施落实方案中技术实施内容和管理措施落实方案中管理实施内容等文档进行整理，形成信息系统安全建设详细设计方案。

安全详细设计方案包含以下内容：

- 本期建设目标和建设内容；
- 技术实现框架；
- 信息安全产品或组件功能及性能；

- 信息安全产品或组件部署；
- 安全策略和配置；
- 配套的安全管理建设内容；
- 工程实施计划；
- 项目投资概算。

活动输出：安全详细设计方案。

3）管理措施实现

（1）管理机构和人员的设置

活动目标：本阶段活动的目标是建立配套的安全管理职能部门，通过管理机构的岗位设置、人员的分工以及各种资源的配备为信息系统的安全管理提供组织上的保障。

参与角色：信息系统运营、使用单位，信息安全服务机构。

活动输入：机构现有相关管理制度和政策、安全详细设计方案。

活动描述：本活动主要包括以下子活动内容。

- 安全组织的确定：识别与信息安全管理有关的组织成员及其角色，例如操作人员、文档管理员、系统管理员、安全管理员等，形成安全组织结构表。
- 角色说明：以书面的形式详细描述每个角色与职责，确保所有的风险都有人负责。

活动输出：机构、角色与职责说明书。

（2）管理制度的建立和修订

活动目标：本阶段活动的目标是建立或修订与信息系统安全管理相配套的包括所有信息系统的建设、开发、运维、升级和改造等各个阶段和环节应当遵循的行为规范和操作规程。

参与角色：信息系统主管部门，信息系统运营、使用单位，信息安全服务机构。

活动输入：安全组织结构表、安全成员及角色说明书、安全详细设计方案。

活动描述：本活动主要包括以下子项内容。

- 明确适用范围：建立的管理制度首先要明确制度的应用范围，如机房管理、账户管理、远程访问管理、特殊权限管理、设备管理、变更管理等方面的内容。
- 定义人员职责：建立的管理制度要明确相关岗位人员的责任和权力范围，并要征求相关人员的意见，确保责任主体明确。
- 规定行为规范：建立的管理制度要通过制度化、规范化和流程化的行为来保证各项管理工作的一致性。
- 评估与完善：建立的管理制度在发布、执行过程中要定期进行评估，根据实际运行环境和信息系统的变化对制度进行修改和完善，必要时要考虑重新制定管理制度。

活动输出：各项管理制度和操作规范。

（3）人员安全技能培训

活动目标：本阶段活动的目标是对人员的职责、素质、技能等方面进行培训，保证人员具有与其岗位职责相适应的技术能力和管理能力，以减少人为因素给系统带来的安全风险。

参与角色：信息系统主管部门，信息系统运营、使用单位，信息安全服务机构。

活动输入：系统/产品使用说明书、各项管理制度和操作规范。

活动描述：针对普通员工、管理员、开发人员、主管人员以及安全人员的特定技能培训和安全意识培训，培训后进行考核，合格者发给上岗资格证书等。

活动输出：培训记录及上岗资格证书等。

（4）安全实施过程的管理

活动目标：本阶段活动的目标是在系统定级、规划设计、实施过程中对工程的质量、进度、文档和变更等方面的工作进行监督控制和科学管理。

参与角色：信息系统运营、使用单位，信息安全服务机构，信息安全产品供应商。

活动输入：安全设计与实施阶段参与各方的相关进度控制和质量监督要求文档。

活动描述：本活动主要包括以下子项内容。

- 质量管理：质量管理首先要控制系统建设的质量，保证系统建设始终在等级保护制度所要求的框架内进行，同时还要保证用于创建系统的过程的质量。在系统建设的过程中，要建立一个不断测试和改进质量的过程。在整个系统的生命周期中，通过测试、分析和修正活动保证所完成目标和过程的质量。
- 风险管理：识别、评估和降低风险，以保证系统工程活动和全部技术工作项目都成功实施。在整个系统建设过程中，风险管理要贯穿始终。
- 变更管理：在系统建设的过程中，由于各种信息系统本身和运行环境条件等的变化会导致变更的出现，变更发生在工程的范围、进度、质量、费用、人力资源、沟通、合同等多方面。每一次的变更处理必须遵循同样的程序，即相同的文字报告、相同的管理办法、相同的监控过程，必须确定每一次变更对系统成本、进度、风险和技术要求的影响，一旦批准变更，必须按照设定的规程来执行变更。
- 进度管理：系统建设各阶段的实施必须有一组明确的可交付成果的指标，同时要求有结束的日期，因此在建设系统的过程中必须制订项目进度计划，绘制路线图，将系统分解为不同的子任务，并进行时间控制确保项目如期完成。
- 文档管理：文档是记录项目整个过程的书面资料，在系统建设的过程中，针对每个环节都有大量的文档输出，文档管理涉及系统建设的各个环节，主要包括系统定级、规划设计、方案设计、安全实施、系统验收、人员培训等方面。

活动输出：各阶段管理过程文档。

4）技术措施实现

（1）信息安全产品采购

活动目标：本阶段活动的目标是按照安全详细设计方案中对安全产品的具体功能/性能指标要求，根据备选产品或产品组合实现的功能，在满足安全设计要求的前提下选购所需的信息安全产品。

参与角色：信息安全产品供应商，信息系统运营、使用单位。

活动输入：安全详细设计方案、相关产品信息。

活动描述：本活动主要包括以下子项内容。

- 制定产品采购说明书：信息安全产品的选型过程首先依据安全详细设计方案的设计要求制定产品采购说明书，对产品的采购原则、采购范围、指标要求、采购方式、采购流程等方面进行说明，然后依据产品采购说明书对现有产品进行比对和筛选。对于产品的功能和性能指标，可以依据国家认可的测试机构所出具的产品测试报告，也可以依据用户自行组织的信息安全产品功能和性能选型测试所出具的报告。
- 产品选择：在依据产品采购说明书对现有产品进行选择时，不仅要考虑产品的使用

环境、安全功能、成本(包括采购和维护成本)、易用性、可扩展性、与其他产品的互动和兼容性等因素,还要考虑产品质量和可信性。产品可信性是保证系统安全的基础,用户在选择信息安全产品时应确保符合国家关于信息安全产品使用的有关规定。对于密码产品的使用,应当按照国家密码管理的相关规定进行选择和使用。

活动输出:需采购信息安全产品清单。

(2) 安全设备开发

活动目标:本阶段活动的目标是对一些不能通过采购现有信息安全产品来实现的安全措施和安全功能通过专门的设计、开发来实现。安全设备的开发应当与系统的应用开发同步设计、同步实施,而应用系统一旦开发完成后,再增加安全措施或需要将安全机制潜入应用系统时会造成很大的额外成本投入,因此,在应用系统开发的同时要依据安全详细设计方案进行安全技术或机制的开发设计,保证系统应用与安全设备同步建设。

参与角色:信息系统运营、使用单位,信息安全服务机构。

活动输入:安全详细设计方案。

活动描述:本活动主要包括以下子项内容。

- 安全措施需求分析:以规范的形式准确表达安全方案设计中的指标要求,确定软件设计的约束和软件同其他系统相关的接口细节。
- 概要设计:概要设计要考虑安全方案中关于身份鉴别、访问控制、安全审计、通信完整性、通信保密性、抗抵赖等方面的指标要求,设计安全措施模块的体系结构,定义安全设备的模块组成,定义每个模块的主要功能和模块之间的接口。
- 详细设计:依据概要设计说明书将安全设备开发进一步细化,对每个安全功能模块的接口、初始化参数要求、各接口之间的关系、各部分的内在实现机理都要进行详细的分析和设计。

按照功能需求和模块划分进行各个部分的详细设计,包含接口设计和管理方式设计等。详细设计是设计人员根据概要设计书进行的模块设计,将总体设计所获得的模块按照单元、程序、过程的顺序逐步细化,详细定义各个单元的数据结构、程序的实现算法以及程序、单元、模块之间的接口等,作为以后编码工作的依据。

- 编码实现:按照设计进行硬件调试和软件的编码,在编码和开发过程中要关注硬件组合的安全性和编码的安全性,并通过论证和测试。
- 测试:开发基本完成后要进行测试,保证功能的实现和安全性的实现。测试分为单元测试、集成测试、系统测试和以用户试用为主的用户测试 4 个步骤。
- 安全设备开发过程文档化:安全设备开发过程需要将概要设计说明书、详细设计说明书、开发测试报告以及开发说明书等整理归档。

活动输出:安全设备开发过程相关文档。

(3) 安全集成

活动目标:本阶段活动的目标是将不同的软/硬件产品集成起来,依据安全详细设计方案将信息安全产品、系统软件平台和开发的安全控制模块与各种应用系统综合、整合成为一个系统。安全控制集成的过程需要把安全实施、风险控制、质量控制等有机地结合起来,遵循运营、使用单位与信息安全服务机构共同参与、相互配合的实施原则。

参与角色:信息系统运营、使用单位,信息安全服务机构。

活动输入：安全详细设计方案。

活动描述：本活动主要包括以下子项内容。

- 制定集成实施方案：主要工作内容是制定安全集成实施方案，安全集成实施方案的目标是具体指导工程的建设内容、方法和规范等，实施方案有别于安全设计方案的一个显著特征就是它的可操作性很强，要具体落实到产品的安装、部署和配置中，安全集成实施方案是工程建设的具体指导文件。
- 实施安全集成前的准备：主要工作内容是对实施环境进行准备，包括硬件设备准备、软件系统准备、环境准备。为了保证安全集成系统实施的质量，信息安全服务机构应该依据系统设计方案制定一套可行的系统质量控制方案，以便有效地指导安全集成系统的实施过程。该质量控制方案应该确定系统实施各个阶段的质量控制目标、控制措施、工程质量问题的处理流程、系统实施人员的职责要求等，并提供详细的安全集成进度表。
- 安全集成的实施：主要工作内容是将配置好策略的信息安全产品和模块部署到实际的应用环境中，并调整相关策略。安全集成实施应严格按照集成进度安排进行，出现问题各方应及时沟通。系统实施的各个环节应该遵照质量控制方案的要求分别进行系统测试，逐步实现质量控制目标。例如在综合布线系统施工过程中应该及时利用网络测试仪测定线路质量，及早发现并解决质量问题。
- 培训：信息系统建设完成后，安全服务提供商应当向运营和使用单位提供信息系统使用说明书及建设过程文档，同时需要对系统维护人员进行必要的培训，培训效果的好坏将直接影响到今后系统能否安全运行。
- 形成安全集成报告：应将安全集成过程相关内容文档化，并形成安全集成报告，其中包含集成实施方案、质量控制方案、集成实施报告以及培训考核记录等内容。

活动输出：安全集成报告。

（4）系统验收

活动目标：本阶段活动的目标是检验系统是否严格按照安全详细设计方案进行建设，是否实现了设计的功能和性能。在安全集成工作完成后，系统测试及验收是从总体出发对整个系统进行集成性的安全测试，包括对系统运行效率和可靠性的测试，也包括对管理措施落实内容的验收。

参与角色：信息系统主管部门，信息系统运营、使用单位，信息安全服务机构。

活动输入：安全详细设计方案、安全控制集成报告。

活动描述：本活动主要包括以下子项内容。

- 集成系统验收前的准备：安全设备开发、集成完成后要根据安全设计方案中需要达到的安全目标准备系统验收方案。系统验收方案应当以合同条款、需求说明书和安全设计方案为参照依据，充分体现用户的安全需求。
- 成立系统验收工作组对验收方案进行审核，组织制定验收计划、定义验收的方法和严格程度。
- 组织系统验收：由系统验收工作组按照验收计划负责组织实施，组织测试人员根据已通过评审的系统验收方案对系统进行测试。
- 验收报告：在测试完成后形成验收报告，验收报告需要用户与建设方进行确认。验

收报告将明确给出验收的结论(其中包括需要修改或改善的内容),安全服务提供商应当根据验收意见尽快修正有关问题,重新进行验收或者转入合同争议处理程序。

- 安全集成系统交付：在系统验收通过以后要进行系统的交付,需要安全服务提供商提交系统建设过程中的文档、指导用户进行系统运行维护的文档、服务承诺书等。

活动输出：安全集成系统验收报告。

4. 安全运行与维护

1）安全运行与维护阶段的工作流程

安全运行与维护是等级保护实施过程中确保信息系统正常运行的必要环节,涉及的内容较多,包括安全运行与维护机构和安全运行与维护机制的建立,环境、资产、设备、介质的管理,网络、业务应用系统的管理,密码、密钥的管理,运行、变更的管理,安全状态监控和安全事件处置,安全审计和安全检查等内容。此处并不对上述所有管理过程的具体操作内容和方法进行描述,希望全面了解和控制安全运行与维护阶段各类过程中具体操作内容和方法的读者可以参见其他标准或指南,例如 GB/T 20988—2007《信息安全技术　信息系统灾难恢复规范》、GB/Z 20986—2007《信息安全技术　信息安全事件分类分级指南》、GB/Z《20985—2007 信息技术　安全技术　信息安全事件管理指南》等,此处只对安全运行和维护阶段的各个环节的管理目标和流程进行描述。

安全运行与维护阶段的运行管理和控制、变更管理和控制、安全状态监控、安全事件处置和应急预案、安全检查和持续改进以及监督检查等过程的工作流程见图 4.6。

2）运行管理和控制

(1) 运行管理职责的确定

活动目标：本阶段活动的目标是对运行管理活动或任务的角色进行划分,并授予相应的管理权限,以此确定安全运行管理的具体人员和职责。

参与角色：信息系统运营、使用单位。

活动输入：安全详细设计方案、安全组织机构表。

活动描述：本活动主要包括以下子项内容。

- 划分运行管理角色：根据管理制度和实际运行管理需求划分运行管理需要的角色,越高的安全保护等级的运行管理角色的划分越细。
- 授予管理权限：根据管理制度和实际运行管理需要授予每一个运行管理角色不同的管理权限,安全保护等级越高的系统管理权限的划分越细。
- 定义人员职责：根据不同的安全保护等级要求的控制粒度分析所需要运行管理控制的内容,并以此定义不同运行管理角色的职责。

活动输出：运行管理人员的角色和职责表。

(2) 运行管理过程控制

活动目标：本阶段活动的主要目标是通过制定运行管理操作规程确定运行管理人员的操作目的、操作内容、操作时间和地点、操作方法和流程等,并进行操作过程记录,确保对操作过程进行控制。

参与角色：信息系统运营、使用单位。

活动输入：运行管理需求、运行管理人员角色和职责表。

活动描述：本活动主要包括以下子项内容。

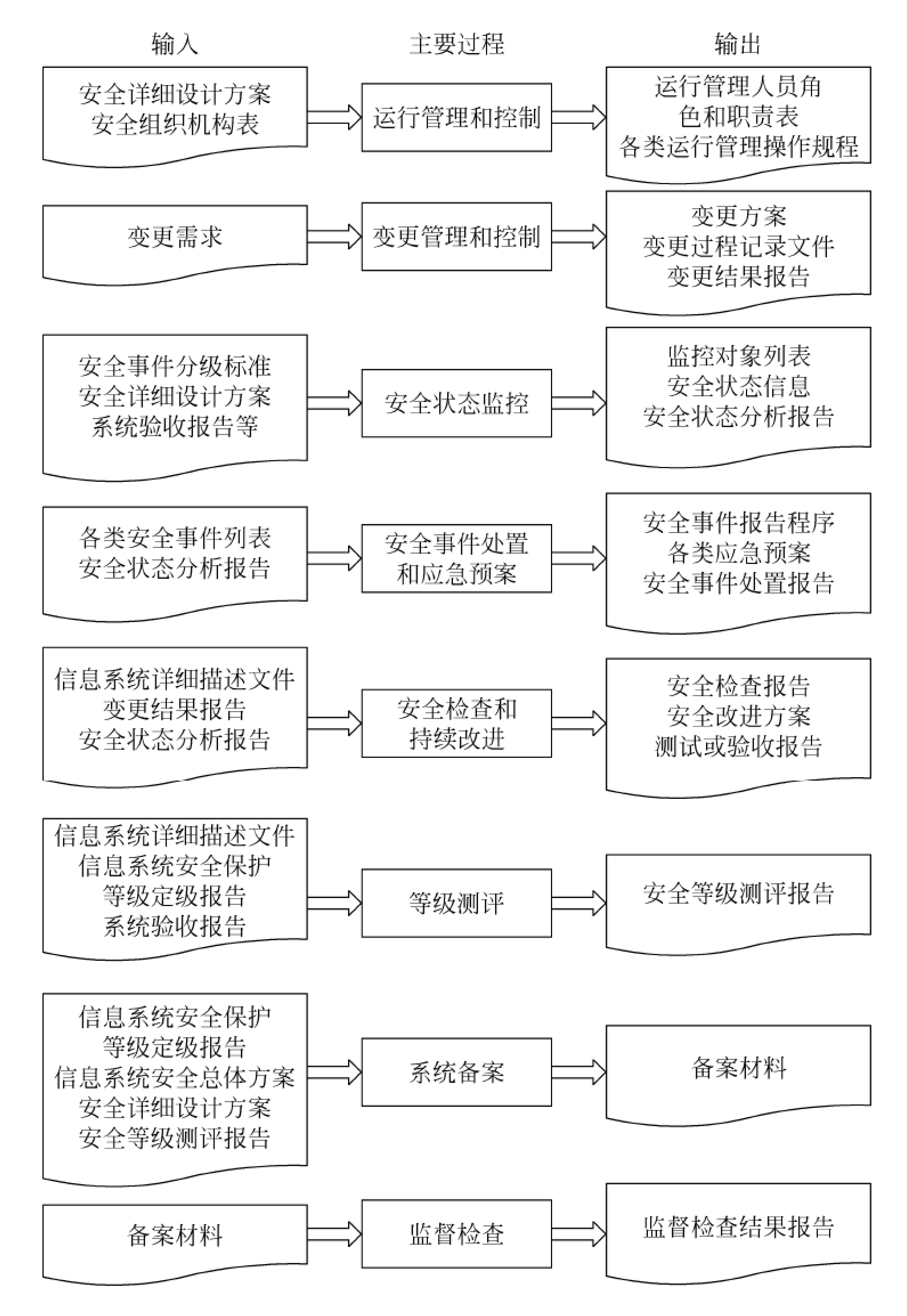


图 4.6　安全运行与维护阶段的主要过程

- 建立操作规程：将操作过程或流程规范化，并形成指导运行管理人员工作的操作规程作为规范操作行为的正式文件。
- 操作过程记录：对运行管理人员按照操作规程执行的操作过程形成相关的记录文件，可能是日志文件，记录操作的时间和人员、正常或异常等信息。

活动输出：各类运行管理操作规程。

3）变更管理和控制

（1）变更需求和影响分析

活动目标：本阶段活动的主要目标是通过对变更需求和变更影响的分析来确定变更的类别，并计划后续的活动内容。

参与角色：信息系统运营、使用单位。

活动输入：变更需求。

活动描述：本活动主要包括以下子项内容。

- 变更需求分析：对变更需求进行分析，确定变更的内容、变更资源需求和变更范围等，判断变更的必要性和可行性。
- 变更影响分析：对变更可能引起的后果进行判断和分析，确定可能产生的影响大小，进行变更的先决条件和后续活动等。
- 明确变更的类别：确定信息系统是局部调整还是重大变更，如果是由信息系统类型发生变化、承载的信息资产类型发生变化、信息系统服务范围发生变化和业务处理自动化程度发生变化等原因引起信息系统安全保护等级发生变化的重大变更，则需要重新确定信息系统安全保护等级，返回到等级保护实施过程的信息系统定级阶段；如果是局部调整，则需要确定配套进行的其他工作内容。
- 制定变更方案：根据上述子项活动的结果制定变更方案。

活动输出：变更方案。

（2）变更过程控制

活动目标：本阶段活动的目标是确保变更实施过程受到控制，各项变化内容必须进行记录，保证变更对业务的影响最小。

参与角色：信息系统运营、使用单位。

活动输入：变更方案。

活动描述：本活动主要包括以下子项内容。

- 变更内容的审核和审批：对变更目的、内容、影响、时间和地点以及人员权限进行审核，以确保变更合理、科学的实施，按照机构建立的审批流程对变更方案进行审批。
- 建立变更过程日志：按照批准的变更方案实施变更，对变更过程中各类系统状态、各种操作活动等建立操作记录或日志。
- 形成变更结果报告：收集变更过程的各类相关文档，整理、分析和总结各类数据，形成变更结果报告，并归档保存。

活动输出：变更结果报告。

4）安全状态监控

（1）监控对象的确定

活动目标：本阶段活动的目标是确定可能会对信息系统安全造成影响的因素，即确定安全状态监控的对象。

参与角色：信息系统运营、使用单位。

活动输入：安全详细设计方案、系统验收报告等。

活动描述：本活动主要包括以下子项内容。

- 安全关键点分析：对影响系统、业务安全性的关键要素进行分析，确定安全状态监控的对象，这些对象可能包括防火墙、入侵检测、防病毒、核心路由器、核心交换机、主要通信线路、关键服务器或客户端等系统范围内的实体，也可能包括安全标准和法律法规等外部对象。
- 形成监控对象列表：根据确定的监控对象分析监控的必要性和可行性、监控的开销和成本等因素，形成监控对象列表。

活动输出：监控对象列表。

(2) 监控对象状态信息的收集

活动目标：本活动的目标是选择状态监控工具，收集安全状态监控的信息，识别和记录入侵行为，对信息系统的安全状态进行监控。

参与角色：信息系统运营、使用单位。

活动输入：监控对象列表。

活动描述：本活动主要包括以下子项内容。

- 选择监控工具：根据监控对象的特点、监控管理的具体要求、监控工具的功能和性能特点等选择合适的监控工具。监控工具也可能不是单一的自动化工具，而只是由各类人员构成的遵循一定规则进行操作的组织，或者是两者的综合。
- 状态信息的收集：收集来自监控对象的各类状态信息，可能包括网络流量、日志信息、安全报警和性能状况等，或者是来自外部环境的安全标准和法律法规的变更信息。

活动输出：安全状态信息。

(3) 监控状态分析和报告

活动目标：本阶段活动的目标是通过对安全状态信息进行分析，及时发现安全事件或安全变更需求，并对其影响程度和范围进行分析，形成安全状态结果分析报告。

参与角色：信息系统运营、使用单位。

活动输入：安全状态信息。

活动描述：本活动主要包括以下子项内容。

- 状态分析：对安全状态信息进行分析，及时发现险情、隐患或安全事件，并记录这些安全事件，分析其发展趋势。
- 影响分析：分析安全状况的变化对整体安全的影响，以决定是否有必要作出响应。
- 形成安全状态分析报告：根据安全状态分析和影响分析的结果形成安全状态分析报告，上报安全事件或提出变更需求。

活动输出：安全状态分析报告。

5) 安全事件处置和应急预案

(1) 安全事件的分级

活动目标：本阶段活动的目标是结合信息系统的实际情况分析安全事件对信息系统的破坏程度、所造成后果的严重程度，将安全事件的破坏程度进行分级。

参与角色：信息系统运营、使用单位。

活动输入：各类安全事件列表。

活动描述：本活动主要包括以下子项内容。

- 安全事件调查和分析：针对各类安全事件列表调查本系统内安全事件的类型、安全事件对业务的影响范围和程度，以及安全事件所涉及的受侵害客体的敏感程度等信息，分析对安全事件进行响应恢复所需要的时间。
- 安全事件的等级划分：根据以上调查和分析结果、根据信息安全事件造成的损失程度、信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定事件等级，制定安全事件的报告程序。

活动输出：安全事件报告程序。

(2) 应急预案的制定

活动目标：本阶段活动的目标是通过对安全事件的等级分析，在统一的应急预案框架下制定对不同等级安全事件的应急预案。

参与角色：信息系统运营、使用单位。

活动输入：安全事件报告程序。

活动描述：本活动主要包括以下子项内容。

- 确定应急预案对象：针对安全事件等级考虑其发生可能性及对系统和业务产生的影响，确定需制定应急预案的安全事件对象。
- 确定和认可各项职责：在统一的应急预案框架下明确和认可应急预案中各部门的职责，并协调各部门间的分工和合作。
- 制定应急预案程序及其执行条件：针对不同等级、不同优先级的安全事件制定相应的应急预案程序，确定安全事件的响应和处置范围、程度以及适用的管理制度，说明应急预案启动的条件，发生安全事件后要采取的流程和措施，并按照预案定期开展演练。

活动输出：各类应急预案。

(3) 安全事件处置

活动目标：本阶段活动的目标是对监控到的安全事件采取适当的方法进行处置，对安全事件的影响程度和等级进行分析，确定是否启动应急响应。

参与角色：信息系统运营、使用单位。

活动输入：安全状态分析报告、安全事件报告程序、各类应急预案。

活动描述：本活动主要包括以下子项内容。

- 安全事件上报：根据安全状态分析报告分析可能的安全事件，对接报的安全事件进行分析，确定安全事件等级、影响程度以及优先级等，按照安全事件报告程序上报安全事件，确定是否应对安全事件启动应急预案。
- 安全事件处置：对于应该启动应急预案的安全事件，按照应急预案响应机制进行安全事件处置。对未知安全事件的处置应根据安全事件的等级制定安全事件处置方案，包括安全事件处置方法以及应采取的措施等，并按照安全事件处置流程和方案对安全事件进行处置。
- 安全事件总结和报告：一旦安全事件得到解决，对于未知的安全事件进行事件记录，分析记录信息并补充所需信息，使安全事件成为已知事件，并文档化；对安全事件处置过程进行总结，制定安全事件处置报告，并保存。

活动输出：安全事件处置报告。

6) 安全检查和持续改进

(1) 安全状态检查

活动目标：本阶段活动的主要目标是通过对信息系统的安全状态进行检查，为信息系统的持续改进过程提供依据和建议，确保信息系统的安全保护能力满足相应等级安全要求。

参与角色：信息系统主管部门，信息系统运营、使用单位。

活动输入：信息系统详细描述文件、变更结果报告、安全状态分析报告。

活动描述：本活动主要包括以下子项内容。

- 确定检查对象和检查方法：确定检查的目标和意义，确定本次安全检查活动是自己组织的检查还是他方组织的安全检查，如果是他方组织的安全检查，则需要与他方实施检查的单位进行沟通和配合。
- 制定检查计划和检查方案：确定检查工作的角色和职责，确定检查工作的方法，成立安全检查工作组，制定安全检查工作计划和安全检查方案，说明安全检查的范围、对象、工作方法等，准备安全检查需要的各类表单和工具。
- 安全检查实施：根据安全检查计划通过询问、检查和测试等多种手段进行安全状况检查，记录各种检查活动的结果数据，分析安全措施的有效性、安全事件发生的可能性和信息系统的实际改进需求等。
- 安全检查结果和报告：总结安全检查的结果，提出改进的建议，并产生安全检查报告，将安全检查过程中的各类文档、资料归档保存。

活动输出：安全检查报告。

(2) 改进方案的制定

活动目标：本阶段活动的主要目标是依据安全检查的结果调整信息系统的安全状态，保证信息系统安全防护的有效性。

参与角色：信息系统运营、使用单位。

活动输入：安全检查报告。

活动描述：本活动主要包括以下子项内容。

- 安全改进的立项：根据安全检查结果确定安全改进的策略，如果涉及安全保护等级的变化，则应进入安全保护等级保护实施的一个新的循环过程；如果安全保护等级不变，但是调整内容较多、涉及范围较大，则应对安全改进项目进行立项，重新开始安全实施/实现过程；如果调整内容较少，则可以直接进行安全改进实施。
- 制定安全改进方案：确定安全改进的工作方法、工作内容、人员分工、时间计划等，制定安全改进方案。安全改进方案只适用于小范围内的安全改进，例如安全加固、配置加强、系统补丁等。

活动输出：安全改进方案。

(3) 安全改进的实施

活动目标：本阶段活动的目标是保证按照安全改进方案实现各项补充安全措施，并确保原有的技术措施和管理措施与各项补充的安全措施一致有效地工作。

参与角色：信息系统运营、使用单位。

活动输入：安全改进方案。

按照安全改进方案实施和落实各项补充的安全措施后，要调整和修订各类相关的技术文件和管理制度，保证原有体系的完整性和一致性。

活动输出：测试或验收报告。

7) 等级测评

活动目标：本阶段活动的目标是通过信息安全等级测评机构对已经完成等级保护建设的信息系统定期进行等级测评，确保信息系统的安全保护措施符合相应等级的安全要求。

参与角色：信息系统主管部门，信息系统运营、使用单位，信息安全等级测评机构。

活动输入：信息系统详细描述文件、信息系统安全保护等级定级报告、系统验收报告。

活动描述：参见有关信息系统安全保护等级测评的规范或标准，可以在“http://www.cspec.gov.cn/”查阅。

活动输出：安全等级测评报告。

8）系统备案

活动目标：本阶段活动的目标是根据国家管理部门对备案的要求整理相关备案材料，并向受理备案的单位提交备案材料。

参与角色：信息系统主管部门，信息系统运营、使用单位，国家管理部门。

活动输入：信息系统安全保护等级定级报告、信息系统安全总体方案、安全详细设计方案、安全等级测评报告。

活动描述：本活动主要包括以下子项内容。

- 备案材料的整理：信息系统运营、使用单位针对备案材料的要求整理、填写备案材料；
- 备案材料的提交：信息系统运营、使用单位根据国家管理部门的要求办理定级备案手续，提交备案材料；国家管理部门接收备案材料。

活动输出：备案材料。

9）监督检查

活动目标：本活动的目标是通过国家管理部门对信息系统定级、规划设计、建设实施和运行管理等过程进行监督检查，确保其符合信息系统安全保护等级相应的要求。

参与角色：信息系统主管部门，信息系统运营、使用单位，国家管理部门。

活动输入：备案材料。

活动描述：参见信息安全等级保护监督检查的规范或标准，可以在“http://www.cspec.gov.cn/”查阅。

活动输出：监督检查结果报告。

5. 信息系统终止

1）信息系统终止阶段的工作流程

信息系统终止阶段是等级保护实施过程中的最后环节。当信息系统被转移、终止或废弃时，正确处理系统内的敏感信息和残留的敏感信息对于确保机构信息资产的安全是至关重要的。在信息系统生命周期中，有些系统并不是真正意义上的废弃，而是改进技术或将业务转移到新的信息系统，对于这些信息系统，在终止处理过程中应确保信息转移、设备迁移和介质销毁等方面的安全。

信息系统终止阶段涉及的信息转移、暂存和清除，设备迁移或废弃，存储介质的清除或销毁等活动的工作流程见图 4.7。

2）信息转移、暂存和清除

活动目标：本阶段活动的目标是在信息系统终止处理过程中，对于可能会在另外的信息系统中使用的信息采取适当的方法将其安全地转移或暂存到可以恢复的介质中，确保将来可以继续使用，同时采用安全的方法清除要终止的信息系统中的信息。

参与角色：信息系统运营、使用单位。

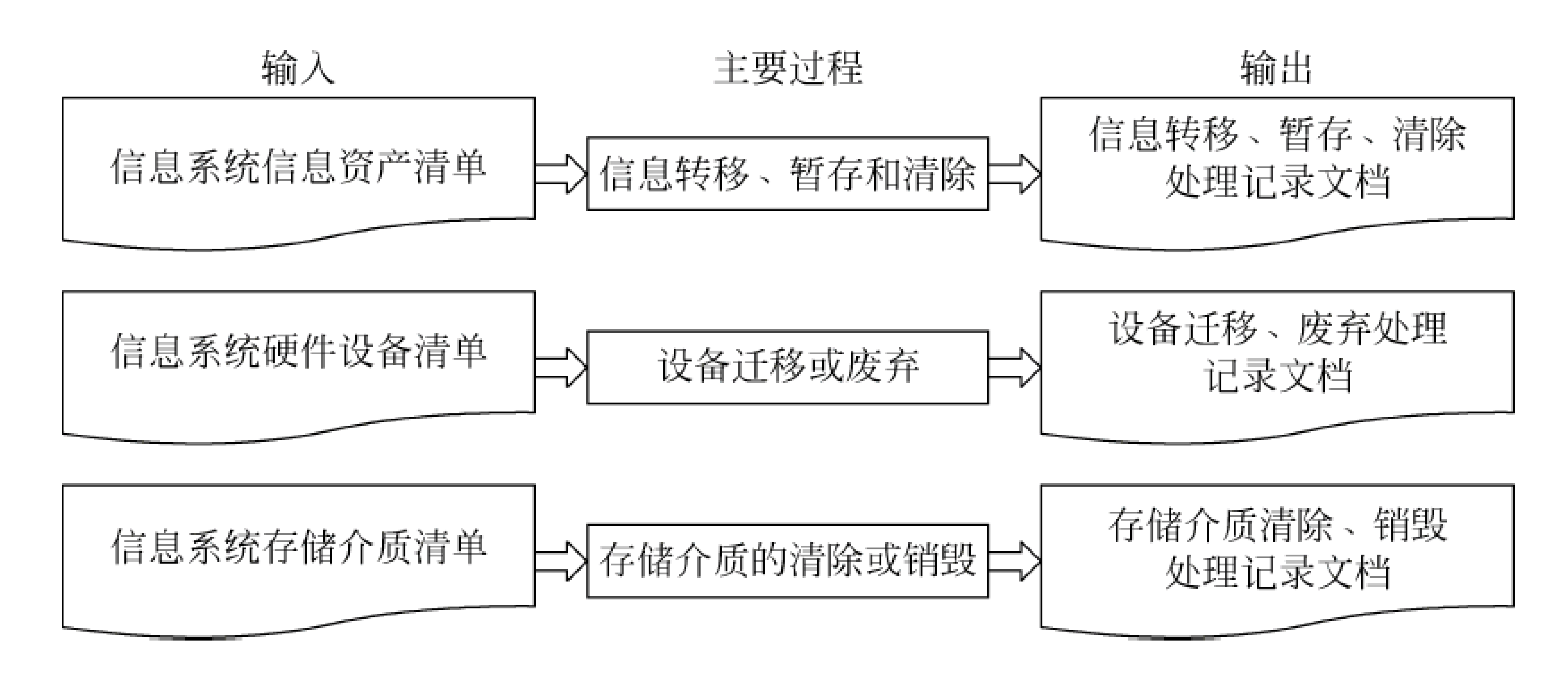


图 4.7 信息系统终止阶段的工作流程

活动输入：信息系统信息资产清单。

活动描述：本活动主要包括以下子项内容。

- 识别要转移、暂存和清除的信息资产：根据要终止的信息系统的信息资产清单识别重要信息资产、所处的位置以及当前状态等，列出需转移、暂存和清除的信息资产的清单。
- 信息资产转移、暂存和清除：根据信息资产的重要程度制定信息资产的转移、暂存、清除的方法和过程。如果是涉密信息，应该按照国家相关部门的规定进行转移、暂存和清除。
- 处理过程记录：记录信息转移、暂存和清除的过程，包括参与的人员，转移、暂存和清除的方式以及目前信息所处的位置等。

活动输出：信息转移、暂存、清除处理记录文档。

3）设备迁移或废弃

活动目标：本活动的目标是确保信息系统终止后迁移或废弃的设备内不包括敏感信息，对设备的处理方式应符合国家相关部门的要求。

参与角色：信息系统运营、使用单位。

活动输入：设备迁移或废弃清单等。

活动描述：本活动主要包括以下子项内容。

- 软/硬件设备识别：根据要终止的信息系统的设备清单识别要被迁移或废弃的硬件设备、所处的位置以及当前状态等，列出需迁移、废弃的设备的清单。
- 制定硬件设备处理方案：根据规定和实际情况制定设备处理方案，包括重用设备、废弃设备、敏感信息的清除方法等。
- 处理方案审批：重用设备、废弃设备、敏感信息的清除方法等的设备处理方案应该经过主管领导审查和批准。
- 设备处理和记录：根据设备处理方案对设备进行处理，如果是涉密信息的设备，其处理过程应符合国家相关部门的规定；记录设备处理过程，包括参与的人员、处理的方式、是否有残余信息的检查结果等。

活动输出：设备迁移、废弃处理报告。

4）存储介质的清除或销毁

活动目标：本阶段活动的目标是通过采用合理的方式对计算机介质（包括磁带、磁盘、

打印结果和文档)进行信息清除或销毁处理,防止介质内的敏感信息泄露。

参与角色:信息系统运营、使用单位。

活动输入:存储介质清单等。

活动描述:本活动主要包括以下子项内容。

- 识别要清除或销毁的介质:根据要终止的信息系统的存储介质清单识别载有重要信息的存储介质、所处的位置以及当前状态等,列出需清除或销毁的存储介质清单。
- 确定存储介质处理方法和流程:根据存储介质所承载信息的敏感程度确定对存储介质的处理方式和处理流程,对存储介质的处理包括数据清除和存储介质销毁等。对于存储涉密信息的介质应按照国家相关部门的规定进行处理。
- 处理方案审批:存储介质的处理方式和处理流程等的处理方案应该经过主管领导审查和批准。
- 存储介质处理和记录:根据存储介质处理方案对存储介质进行处理,记录处理过程,包括参与的人员、处理的方式、是否有残余信息的检查结果等。

活动输出:存储介质的清除或销毁记录文档。

4.2.4 安全等级保护的管理

运营、使用单位应当参照《信息安全技术信息系统安全管理要求》(GB/T 20269—2006)、《信息安全技术信息系统安全工程管理要求》(GB/T 20282—2006)、《信息系统安全等级保护基本要求》等管理规范制定并落实符合本系统安全保护等级要求的安全管理制度。

4.2.4.1 测评

信息系统建设完成或原有信息系统改造或扩充、升级后,均应依据《信息系统安全等级保护测评要求》等技术标准选择符合管理办法规定条件的测评机构进行安全保护等级的测评。在确认其安全保证等级(安全保证等级是对测评结果评价的术语)已达到安全保护等级要求后方可投入运行。

信息系统投入正式运行后,运营、使用单位或其主管部门应定期对信息系统安全保证等级状况开展复核性测评,确定为安全保护等级第三级的信息系统,应当至少每年进行一次安全保护等级的复核性测评;确定为安全保护等级第四级的信息系统,应当至少每半年进行一次安全保护等级的复核性测评;确定为安全保护等级第五级的信息系统,应当依据特殊安全需求定期进行安全保护等级复核性测评。

信息系统投入正式运行后,运营、使用单位及其主管部门应当定期对信息系统的安全保护状况、安全保护制度及措施的落实情况和维护情况进行自查,确定为安全保护等级第三级的信息系统,应当至少每年进行一次自查;确定为安全保护等级第四级的信息系统,应当至少每半年进行一次自查;确定为安全保护等级第五级的信息系统,应当依据特殊安全需求定期进行自查。

经测评或者自查,信息系统安全等级保护状况未达到安全保护等级要求的,运营、使用单位应当制定方案进行整改,确定为安全保护等级第三、第四和第五级信息系统的整改方案应按管理办法遵照安全监管部门的规定报备或报批。

4.2.4.2 备案和审查

1. 备案

新建第二级(含)以上信息系统,在经国家认可的测评机构进行安全保证等级测评并符合安全保护等级的要求后投入运行。运行和使用单位应当在投入运行后30日内由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续,此处的“所在地设区的市级”是指具有设立区级行政机构权力的市级单位。

已运营(运行)的第二级(含)以上信息系统,应当在安全保护等级确定后30日内由其运营、使用单位到所在地设区的市级以上公安机关办理备案手续。

隶属于中央的在京单位,其跨省或者全国统一联网运行并由主管部门统一定级的信息系统由主管部门向公安部办理备案手续,跨省或者全国统一联网运行的信息系统在各地运行、应用的分支系统应当向当地设区的市级以上公安机关备案。

办理信息系统安全保护等级备案手续时应当填写《信息系统安全等级保护备案表》,第三级(含)以上信息系统应当同时提供以下材料:

- 系统拓扑结构及说明;
- 系统所属安全组织的机构和管理制度;
- 信息系统安全保护设施设计实施方案或者改建实施方案;
- 信息系统使用的信息安全产品清单及其认证、销售许可证明;
- 测评机构在测评后出具的符合系统安全保护等级的技术检测评估报告;
- 信息系统安全保护等级专家评审意见;
- 主管部门审核批准信息系统安全保护等级的意见。

2. 备案后的审查与检查

信息系统定级报告备案后,受理的公安机关应当对信息系统的备案情况进行审核,对符合等级保护要求的,应当在收到备案材料之日起的10个工作日内颁发信息系统安全等级保护备案证明;发现不符合管理办法及有关标准的,应当在收到备案材料之日起的10个工作日内通知备案单位予以纠正;发现定级不准的,应当在收到备案材料之日起的10个工作日内通知备案单位重新审核确定保护等级。

运营、使用单位或者主管部门重新确定信息系统等级后,应当按照管理办法向公安机关重新备案。

确定为安全保护等级第三级、第四级的信息系统在备案后,受理备案的公安机关除按前述方法审核备案材料外,还应当对运营、使用单位的信息安全等级保护工作情况进行检查。对第三级信息系统每年至少检查一次,对第四级信息系统每半年至少检查一次,对跨省或者全国统一联网运行的信息系统的检查应当会同其主管部门进行。

确定为安全保护等级第五级的信息系统,应当由国家指定的专门部门进行检查。

公安机关、国家指定的专门部门应当对下列事项进行检查:

- 信息系统安全需求是否发生变化,原定保护等级是否准确;
- 运营、使用单位安全管理制度、措施的落实情况;
- 运营、使用单位及其主管部门对信息系统安全状况的检查情况;
- 系统安全等级测评是否符合要求;
- 信息安全产品使用是否符合要求;

- 信息系统安全整改情况；
- 备案材料与运营、使用单位和信息系统的符合情况；
- 其他应当进行监督检查的事项。

4.2.4.3　常规性监督、检查、指导

1. 检查事项

确定了安全保护等级的信息系统运营、使用单位，应当接受公安机关、国家指定的专门部门对信息系统安全运行状况的监督、检查、指导，按要求定期、如实地向公安机关、国家指定的专门部门提供下列有关信息安全等级保护的信息资料及数据文件：

- 信息系统备案事项的变更情况；
- 安全组织、人员的变动情况；
- 信息安全管理制度、措施的变更情况；
- 信息系统运行状况记录；
- 运营、使用单位及主管部门定期对信息系统安全状况的检查记录；
- 对信息系统开展等级测评的技术测评报告；
- 信息安全产品使用的变更情况；
- 信息安全事件应急预案，信息安全事件应急处置结果报告；
- 信息系统安全建设、整改结果报告。

公安机关检查发现信息系统的安全等级保护状况不符合信息安全等级保护有关管理规范和技术标准的，应当向运营、使用单位发出整改通知。运营、使用单位应当根据整改通知要求按照管理规范和技术标准进行整改，整改完成后应当将整改报告向公安机关备案，必要时，公安机关可以对整改情况组织检查。

2. 资质审查

1）产品资质

确定为安全保护等级第三级以上的信息系统，在选择信息安全产品时应当符合以下条件：

- 产品研制、生产单位是由中国公民、法人投资或者国家投资或者控股的，在中华人民共和国境内具有独立的法人资格；
- 产品的核心技术、关键部件具有我国自主知识产权；
- 产品研制、生产单位及其主要业务、技术人员无犯罪记录；
- 产品研制、生产单位声明没有故意留有或者设置漏洞、后门、木马等程序和功能；
- 对国家安全、社会秩序、公共利益不构成危害；
- 对已列入信息安全产品认证目录的，应当取得国家信息安全产品认证机构颁发的认证证书。

2）测评机构资质

确定为安全保护等级第三级以上的信息系统，在选择测评机构进行安全保证等级测评时，测评机构应当符合下列条件：

- 在中华人民共和国境内注册成立（港澳台地区除外）；
- 由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）；
- 从事相关检测评估工作两年以上，无违法记录；

- 工作人员仅限于中国公民；
- 法人及主要业务、技术人员无犯罪记录；
- 使用的技术装备、设施应当符合国家规定的对信息安全产品的要求；
- 具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度；
- 对国家安全、社会秩序、公共利益不构成威胁。

从事信息系统安全保证等级测评的机构应当履行下列义务：

- 遵守国家有关法律法规和技术标准，提供安全、客观、公正的检测评估服务，保证测评的质量和效果；
- 保守在测评活动中知悉的国家秘密、商业秘密和个人隐私，防范测评风险；
- 对测评人员进行安全保密教育，与其签订安全保密责任书，规定应当履行的安全保密义务和承担的法律责任，并负责检查落实。

4.2.5 涉密信息系统的分级保护管理

涉密信息系统的分级保护框架原则来源于信息系统等级保护的框架，但由于涉密信息系统的特殊的国家属性，其管理的主管机构和安全保护措施的选择都与非涉密信息系统存在很大差别。有鉴于此，为了区别起见，习惯地将涉密信息系统的分等级保护称为分级保护（简称分保）。

参考《信息安全等级保护管理办法》（公通字[2007]43号文件）的规定，涉密信息系统依据国家信息安全等级保护的基本要求，根据国家保密工作部门制定的有关涉密信息系统分级保护的管理规定和技术标准，结合涉密信息系统的实际情况进行保护。涉及国家秘密的信息不得在非涉密信息系统中进行处理，同时非涉密信息系统也不得处理涉及国家秘密的信息。

4.2.5.1 密级划分与系统定级

涉密信息系统按照所处理信息的最高密级，由低到高分为秘密、机密、绝密3个等级。

涉密信息系统建设使用单位应在对系统内的信息进行规范定密的基础上依据BMB 20—2007《涉及国家秘密的信息系统分级保护管理规范》和国家保密标准BMB 17—2006《涉及国家秘密的计算机信息系统分级保护技术要求》将系统内信息的密级最高者确定为系统密级，例如涉密信息系统内有的信息属秘密级，有的属机密级，但整个信息系统的密级应定为机密级。对于包含多个安全域的涉密信息系统，各安全域可以分别确定密级。

信息系统的业务主管部门的保密工作机构和国家保密机构应当监督指导涉密信息系统建设和使用单位准确、合理地进行系统定级。

涉密信息系统建设和使用单位应当将涉密信息系统定级和建设使用情况及时上报业务主管部门的保密工作机构和负责系统审批的保密工作部门备案，并接受保密部门的监督、检查、指导。

4.2.5.2 设计与实施的管理

涉密信息系统建设和使用单位应当选择具有涉密集成资质的单位承担或参与涉密信息系统的设计与实施，涉密集成资质由国家保密机构或其授权机构按规定进行审批和年检。

涉密信息系统建设和使用单位应当依据涉密信息系统分级保护管理规范和技术标准，

按照秘密、机密、绝密 3 个等级的不同要求，结合系统实际进行方案设计，实施分级保护，其保护水平总体上分别不低于国家信息安全等级保护第三级、第四级、第五级的水平。

涉密信息系统选用的信息安全保密技术产品原则上应当是国产产品，这些产品应当通过国家保密局授权的检测机构依据国家有关保密技术标准进行的检测，通过检测的产品由国家保密局审核后发布产品目录。

涉密信息系统建设和使用单位在系统工程实施结束后，应当向保密工作部门提出申请，由国家保密局授权的系统测评机构依据国家保密标准 BMB 22—2007《涉及国家秘密的计算机信息系统分级保护测评指南》对涉密信息系统进行安全保密测评。

涉密信息系统建设和使用单位在系统投入使用前，应当按照国保发[2007]18 号《涉及国家秘密的信息系统审批管理规定》向所在地设区的市级以上保密工作部门申请进行系统审批，涉密信息系统在通过审批后方可投入使用。已投入使用的涉密信息系统，其建设和使用单位在按照分级保护要求完成系统整改后，应当向保密工作部门备案。

涉密信息系统建设和使用单位在申请系统审批或者备案时应当提交以下材料：

- 系统设计、实施方案及审查论证意见；
- 系统承建单位资质证明材料；
- 系统建设和工程监理情况报告；
- 系统安全保密检测评估报告；
- 系统安全保密组织机构和管理制度情况；
- 其他有关材料。

4.2.5.3　分级保护的常规性管理

国家和地方各级保密工作部门依法对各地区、各部门涉密信息系统分级保护工作实施监督管理，并做好以下工作：

- 指导、监督和检查分级保护工作的开展；
- 指导涉密信息系统建设使用单位规范信息定密，合理确定系统保护等级；
- 参与涉密信息系统分级保护方案论证，指导建设和使用单位做好保密设施的同步规划设计；
- 依法对涉密信息系统集成资质单位进行监督管理；
- 严格进行系统测评和审批工作，监督检查涉密信息系统建设和使用单位分级保护管理制度和技术措施的落实情况；
- 加强涉密信息系统运行中的保密监督检查，对秘密级、机密级信息系统每两年至少进行一次保密检查或者系统测评，对绝密级信息系统每年至少进行一次保密检查或者系统测评；
- 了解掌握各级各类涉密信息系统的管理使用情况，及时发现和查处各种违规违法行为和泄密事件。

涉密信息系统发生涉密等级、连接范围、环境设施、主要应用、安全保密管理责任单位变更时，其建设和使用单位应当及时向负责审批的保密工作部门报告，保密工作部门应当根据实际情况决定是否对其重新进行测评和审批。

涉密信息系统建设和使用单位应当依据国家保密标准 BMB 20—2007《涉及国家秘密的信息系统分级保护管理规范》加强涉密信息系统运行中的保密管理，定期进行风险评估，

消除泄密隐患和漏洞。

4.2.6 安全等级保护中的密码管理

国家密码管理部门对信息安全等级保护的密码实行分类分级管理。根据被保护对象在国家安全、社会稳定、经济建设中的作用和重要程度,被保护对象的安全防护要求和涉密程度,被保护对象被破坏后的危害程度以及密码使用部门的性质等确定密码的等级保护准则。

信息系统运营、使用单位采用密码进行等级保护的,应当遵照国家密码管理局 2007 年颁布的《信息安全等级保护商用密码管理办法》(国密局发[2007]11 号)和《信息安全等级保护商用密码技术要求》等密码管理规定和相关标准。信息系统安全等级保护中密码的配备、使用和管理等应当严格执行国家密码管理的有关规定。

信息系统运营、使用单位应当充分运用密码技术对信息系统进行保护。采用密码对涉及国家秘密的信息和信息系统进行保护的,应报经国家密码管理机构审批,密码的设计、实施、使用、运行维护和日常管理等应当按照国家密码管理有关规定和相关标准执行;采用密码对不涉及国家秘密的信息和信息系统进行保护的,须遵守《商用密码管理条例》和密码分类分级保护有关规定与相关标准,其密码的配备使用情况应当向国家密码管理机构备案。

运用密码技术对信息系统进行系统等级保护建设和整改的,必须采用经国家密码管理机构批准使用或者准予销售的密码产品进行安全保护,不得采用国外引进或者擅自研制的密码产品;未经批准不得采用含有加密功能的进口信息技术产品。

信息系统中的密码及密码设备的测评工作由国家密码管理机构认可的测评机构承担,其他任何部门、单位和个人不得对密码进行评测和监控。

各级密码管理部门可以定期或者不定期对信息系统等级保护工作中密码配备、使用和管理的情况进行检查和测评,对重要涉密信息系统的密码配备、使用和管理情况每两年至少进行一次检查和测评。在监督检查过程中,发现存在安全隐患或者违反密码管理相关规定或者未达到密码相关标准要求的,应当按照国家密码管理的相关规定进行处置。

4.2.7 安全等级保护管理中的法律责任

《信息安全等级保护管理办法》是我国全面实施信息安全保障极为重要的法规性文件,特别是对涉及国家安全、社会稳定、国计民生等信息系统的安全建设、使用、维护和提供信息安全集成与咨询服务的组织机构以及监管部门具有约束力,必须得到严格执行。

《信息安全等级保护管理办法》明确规定了实施安全等级保护第三级以上(含)的信息系统有关的建设、使用单位的法律责任以及监管部门违反监管纪律的法律责任;参与安全等级保护信息系统设计、实施的信息安全集成单位或受委托协助运行、维护的单位由信息系统的业主与其签订安全责任和保密合同,承担连带的法律责任。

确定为安全保护等级第三级以上(含)信息系统的运营、使用单位违反《信息安全等级保护管理办法》规定的,由公安机关、国家保密工作部门和国家密码工作管理部门按照职责分工责令其限期改正;逾期不改正的,给予警告,并向其上级主管部门通报情况,建议对其直接负责的主管人员和其他直接责任人员予以处理,并及时反馈处理结果。具有下列情况之一的,属于违反《信息安全等级保护管理办法》规定的行为:

- 未按《信息安全等级保护管理办法》规定备案、审批的;

- 未按《信息安全等级保护管理办法》规定落实安全管理制度、措施的；
- 未按《信息安全等级保护管理办法》规定开展系统安全状况检查的；
- 未按《信息安全等级保护管理办法》规定开展系统安全技术测评的；
- 接到相关监管部门要求限期整改的通知后拒不进行整改的；
- 未按《信息安全等级保护管理办法》规定选择使用信息安全产品和测评机构的；
- 未按《信息安全等级保护管理办法》规定如实提供有关文件和证明材料的；
- 违反保密管理规定的；
- 违反密码管理规定的；
- 违反《信息安全等级保护管理办法》其他规定的。

违反上述规定造成严重损害的，由相关部门依照有关法律、法规予以处理。

信息安全监管部门及其工作人员在履行监督管理职责中玩忽职守、滥用职权、徇私舞弊的，依法给予行政处分；构成犯罪的，依法追究刑事责任。

4.3　信息安全管理的指导原则

4.3.1　指导方针和策略原则

我国信息安全管理的指导方针和策略原则遵从《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27 号文)规定，要点如下：

1. 以安全保发展，在发展中求安全

信息安全的目的是通过保护信息系统内有价值的资产，比如数据、硬件、软件和环境等，保证信息系统健康、有序和稳定的运行，促进社会、经济、政治和文化的发展。没有安全保证的信息化，以及牺牲信息化发展来换取安全，是两种必须摒弃的极端做法。科学的安全发展观是在安全意识上全面提高对信息安全保障认识的同时采用渐进的适度安全策略保证和推进信息化的发展，并通过信息化的发展为信息安全保障体系的逐步完善提供充足的人力、财力和物力支持。

2. 受保护资源的价值与保护成本平衡

信息安全的成本和绩效比应该对货币和非货币两方面进行评估，以保证将成本控制在预期的范围内。

3. 明确国家、企业和个人对信息安全的职责和可确认性

应该明确信息系统有关各方(所有者、管理者、经营者、供应商以及使用者)各自应该承担的安全职责和可确认性。

4. 信息安全需要积极防御和综合防范

信息安全必须坚持综合治理的方法，坚持保护与监管相结合、技术措施与管理并重的方针，综合治理方法必须贯穿信息系统的整个生命周期。

5. 定期评估信息系统的残留风险

信息系统及其运行环境是动态变化的，一劳永逸的信息系统安全解决方案是不存在的，因此必须定期评估信息系统的残留风险，并依此调整安全策略和安全措施，以适应动态变化的安全形势。

6. 综合考虑社会因素对信息安全的制约

信息安全受到很多社会因素的制约,比如国家法律、风俗文化和社会影响等。安全措施的选择和实现还应该综合考虑法律框架下信息系统所有者与使用者、所有者和社会各方面之间的利益平衡。

7. 信息安全管理应该体现以人为本

信息系统安全管理措施要尽可能体现人性化、社会公平和交换平等的价值观念。

4.3.2 工程原则

为了指导信息安全工程的组织和实施,本节给出了信息安全工程应遵循的基本原则,这些原则可应用于信息系统的安全规划、设计、开发、实施、运行、维护管理和报废处理等各个环节。这些原则简短明了,可分为 6 类,即基本保证、适度安全、实用性和标准化、保护层次化和系统化、降低复杂度和安全设计结构化。

1. 基本保证

- 在进行信息系统安全工程设计前应制定符合本系统实际的安全规划,其中包括安全目标和安全策略;
- 将安全保障作为信息系统设计中不可分割的部分同步进行设计;
- 识别信息及信息系统资产,以此作为风险分析和安全需求分析的对象;
- 合理划分安全域;
- 确保开发者受过软件安全开发和信息安全服务与机制的良好训练;
- 确保信息系统用户的职业道德和安全意识的持续性教育、培训。

2. 适度安全

- 通过对抗、降低、规避和转移风险等方式将风险降低到可接受的水平,不追求绝对安全或过度安全的目标;
- 安全的标志之一是系统的运行和维护可控或可管理;
- 在减小风险、增加成本开销和降低某些操作有效性之间进行折中,避免盲目地和过度地追求安全目标;
- 采用剪裁方式选择适当的安全措施,并使这些安全措施达成具有一致性的逻辑组合,以满足组织的安全需求;
- 保护信源到信宿的通信全程的机密性、完整性和可用性;
- 在必要时自主开发自用品以满足某些特殊的安全需求;
- 预测、预警并对抗、降低、规避和转移各种可能的风险。

3. 实用性和标准化

- 信息系统的通信和应用程序尽可能采用开放的标准化技术或协议,增强可移植性和互操作性;
- 使用便于交流和沟通的公共语言进行安全需求的开发;
- 设计的新技术安全机制或措施要确保系统平稳过渡,并保证局部采用的新技术不会引起系统的全局性调整,或引发新的脆弱点;
- 尽量简化操作,以减少误操作带来新的风险。

4. 保护层次化和系统化

- 识别并预测普遍性故障和脆弱性；
- 实现分层的安全保护(逐层确保没有遗留的脆弱点未被识别)；
- 设计和运行的信息系统对入侵或攻击应具有必要的识别、阻止和对抗能力，以及对故障和遭到攻击后的响应和恢复能力；
- 提供对信息系统各个组成部分(子系统或组件)的体系性安全保护，使信息系统面对预期的威胁具有持续阻止、对抗和恢复能力；
- 对状态和事件进行检测监控，容忍可以接受的风险，拒绝绝对安全的策略；
- 隔离公共可访问资源与关键业务资源，隔离措施根据信息系统的安全等级保护需要可以是物理的或逻辑的；
- 根据信息系统的安全等级保护需要，采用物理的或逻辑的方法将承载信息处理系统的局域网络与公共网络或外部网络进行隔离；
- 设计并实现审计机制，以检测非授权和越权使用系统资源并支持事故调查和责任认定；
- 开发意外事故和安全事件处置或灾难恢复规程，并组织学习和演练。

5. 降低复杂度

- 安全机制或措施力求简单、实用；
- 尽量减少可信计算系统的组件；
- 实现最小访问权控制；
- 消除不必要的安全机制或安全服务的交叉覆盖或冗余；
- 对开机—处理—关机全程进行安全控制。

6. 安全设计结构化

- 通过对物理的和逻辑的安全措施进行合理组合，实现系统安全体系设计的结构优化；
- 所配置的基础性和支撑性安全设施或安全服务措施可由多个安全域共享；
- 对用户和进程使用鉴别技术，以确保在域内和跨域间的访问进程得到控制；
- 对实体进行标识，以确保操作责任的可追究性和可确认性。

4.4 安全过程管理与 OSI 安全管理的关系

4.4.1 安全过程管理

国际标准化组织(International Organization for Standardization，ISO)曾为开放互连系统安全体系结构制定 ISO/IEC 7498-2-1995(Information Processing System-Open Systems Interconnection-Basic Reference Model-Part 2：Security Architecture)的技术标准文件，由我国等同采用为 GB/T 9387.2—1995(信息处理系统开放系统互连基本参考模型 第 2 部分安全体系结构)，这是开放系统互连(Open System Interconnection，OSI)安全管理的理论基础或方法论的指导性技术文件。

各种类型的组织机构和单位在开放互连的网络环境下建立和运行自己的信息系统，并依赖它们处理其管理与业务活动，或提供信息服务。显然，信息及信息系统资源的机密性、

完整性、可用性、不可抵赖性、可确认性和可靠性等特性的缺失会对这些组织造成有形和无形的影响。由于开放互连的网络采用了开放性和标准化的通信和应用协议，一方面为信息系统之间的信息共享和相互交流以及应用程序的可移植性和互操作性提供了技术实现上的方便性；另一方面，也为未授权和越权访问信息资源提供了客观的条件，更为对信息系统心怀敌意的企图留下入侵或攻击的途径，因此必须采取相应的安全技术措施保护信息及信息系统的这些安全特性。

信息系统安全管理是实现和维持信息及信息系统资源适当保护等级的机密性、完整性、可用性、不可抵赖性、可确认性和可靠性的一个过程。信息系统安全管理的内容包括分析系统资产（的分布），分析针对系统资产的风险，确定安全需求，制定满足这些安全需求的安全策略，依照过程管理的方法对信息系统生命周期的安全进行管理。信息系统安全管理行为或活动主要包括以下方面：

- 制定信息安全规划，决定组织的信息系统安全目标、方针和策略；
- 识别信息系统内信息资产的分布情况；
- 识别出信息系统资产中存在的安全脆弱性或缺陷；
- 识别出信息系统资产的安全脆弱性或缺陷面临的安全威胁；
- 评估安全威胁针对安全脆弱性或缺陷可能造成的（有形的和无形的）影响，即产生的后果；
- 综合分析出信息系统面临的风险（风险点分布及风险强度）；
- 确定组织的信息系统安全需求；
- 通过构建管理与技术相结合的积极防御体系来对抗、降低、规避和转移风险；
- 识别信息系统存在的残留风险，并评估这些残留风险的影响；
- 为了了解和掌握信息系统安全保障体系的效能，检测安全措施的实现和运行情况；
- 定期或根据信息系统变化情况周期性地对风险进行全局的或局部的重新评估，并据此调整安全需求和风险管理策略，从管理和技术的结合上修订安全措施，使系统的残留风险是可以接受的，或可以管控的；
- 安全管理活动还应实施对安全事件的及时检测、审计、响应和告警，实现对安全事件的事前预警、事中控制和事后的恢复与责任认定；
- 设计并实施信息系统备份和灾难恢复工程，制定灾难恢复的培训计划并组织演练；
- 开发和实施可提高安全意识的培训计划和教材。

4.4.2 OSI 管理

OSI（Open System Interconnection，开放系统互连）管理包括对开放互连信息系统的故障管理、计账管理、配置管理、性能管理和安全管理 5 个类型的管理活动，这些管理活动并不承担在 OSI 环境中完成网络通信的具体任务，而是对网络通信有关的资源进行监视、控制和协调。

1. 故障管理

故障管理包括对 OSI 环境中的异常网络通信故障进行检测、隔离和纠正。这些故障可能导致开放系统不能实现运行目标，故障或是持续性的，或是暂时的。故障在开放系统运行中作为特殊事件（比如连接中断、传输中出现差错等）处理，故障检测提供识别故障的能力。故障管理实现下列功能：

- 维护和检查故障日志；
- 接收和处理故障检测报告；
- 识别和跟踪故障；
- 实施一系列诊断性测试；
- 隔离故障点或故障区域；
- 纠正故障行为。

2. 计账管理

计账管理是对使用 OSI 环境中资源的费用和资源的耗费情况进行建账，识别使用这些资源的成本和使用情况。计账管理包括下列功能：

- 通知用户所产生的成本和所耗费的资源；
- 设置账单，使账目表和资源的使用情况相关联；
- 使成本与被请求的多种资源相一致，进而实现设定的通信目标。

3. 配置管理

配置管理识别、操作和控制开放互连的信息系统，从开放互连的信息系统中收集并为其提供运行所需的数据。其目的是为系统或组件的初始化、启动、持续性运行或是终止连接服务提供操作数据。配置管理包括下列功能：

- 对控制开放互连信息系统的路由操作进行参数设置；
- 将被管理目标和目标集与其标识(ID)相关联；
- 对被管理目标进行初始化；
- 按需收集开放互连信息系统运行中的当前状况信息；
- 获得开放互连信息系统发生重大变更的说明；
- 对开放互连信息系统的变更进行参数配置。

4. 性能管理

性能管理激活 OSI 环境中的网络资源以及通信活动的效力。性能管理包括下列功能：

- 收集网络资源及通信活动的统计信息；
- 维护和检查关于开放互连信息系统状态的历史记录；
- 自动地和人工辅助地判断开放互连信息系统的性能；
- 为优化性能管理活动变更开放互连信息系统运行模式。

5. 安全管理

安全管理的目的是支持和维持开放互连信息系统中安全功能的策略，其功能如下：

- 创建、修改、删除及控制安全服务和机制；
- 发布安全相关信息；
- 报告安全相关事件。

在本书中，OSI 管理中的安全管理只是信息安全管理中的一部分。

4.4.3 OSI 安全管理

OSI 安全管理包含两方面，与 OSI 有关的安全管理和 OSI 管理自身的安全管理。OSI 安全管理本身并不执行具体应用业务和通信中的安全保障活动，而是通过创建、修改、增减安全服务和机制支持与控制这些应用业务和通信中的安全保障功能。

OSI 安全管理涉及 OSI 安全服务的管理与安全机制的管理。这种管理要求给这些安全服务与机制分配管理信息,并收集与这些服务和机制的运行有关的信息。例如密钥分配,设置行政管理强加的安全参数,报告正常的与异常的事件(审计与跟踪),以及安全服务的激活与停止。安全管理并不保证在调用特定安全服务协议(例如连接请求的参数)中传递与安全有关的信息的安全,这些信息的安全应由安全服务来提供。

由分布式开放系统的行政管理强加的安全策略可以因开放互连信息系统的具体情况有所不同,但 OSI 安全管理应该支持这些策略。

OSI 安全管理活动可分为下面四类:

- 系统安全管理;
- 安全服务管理;
- 安全机制管理;
- OSI 管理的安全管理。

这几类安全管理执行的关键功能概述如下。

1. 系统安全管理

系统安全管理的典型活动包括以下方面:

- 总体安全策略的管理,包括策略一致性的修改与维护;
- 与其他的 OSI 管理功能的相互作用;
- 与安全服务管理和安全机制管理的交互作用;
- 事件处理管理,例如远程报告那些违反系统安全的明显企图,以及对用来触发事件报告的阈值的修改。
- 安全审计管理。
  - 选择将被记录和被远程收集的事件;
  - 授予或取消对所选事件进行审计跟踪日志记录的能力;
  - 审计记录的远程收集;
  - 准备安全审计报告。
- 安全恢复管理。
  - 维护那些用来对确定的或可疑的安全事件作出应急响应的规则;
  - 对远程报告的违规行为或事件予以响应;
  - 安全管理者之间的交互。

2. 安全服务管理

安全服务管理涉及对具体安全服务功能的管理。下列行为是在管理具体安全服务功能时可能执行的典型活动:

- 将特定的安全服务与其满足的一个或多个安全保护的目标关联;
- 指定与维护可供选择的规则(存在可选情况时),用于选取为提供所需安全服务而使用的特定的安全机制;
- 对那些需要事先取得管理层同意的安全服务可用安全机制进行沟通与协调(本地的与远程的,自动的或人工的);
- 通过适当的安全管理行为调用特定的安全服务,例如为系统提供行政管理强加的安全服务;

• 与其他安全服务管理功能和安全机制管理功能的交互。

3. 安全机制管理

安全机制管理涉及密钥管理、加密管理、数字签名管理、访问控制管理、数据完整性管理、鉴别管理、通信业务填充管理、路由选择控制管理以及公证管理等，下面分别予以介绍。

1）密钥管理

• 周期性地产生与所要求的安全保护等级相当的合适密钥；
• 根据访问控制的要求将产生的每个密钥复制给需要的实体；
• 用可靠办法使这些密钥对实开放系统中的实体实例是可用的，或将这些密钥分配给它们。

应该强调的是，某些密钥管理功能将在 OSI 环境之外执行，例如用可靠手段分配密钥。

工作密钥的选取也可以通过访问密钥分配中心来完成，或事先通过管理协议自动地或人工地进行分配。

2）加密管理

• 与密钥管理的交互作用；
• 建立密码参数；
• 密码同步。

加密机制就是使用密码管理和采用协议方式来调用密码算法。

可使用密码算法寄存器或在实体间进行协商，以调用相同的密码算法。

3）数字签名管理

数字签名管理可以包括以下方面：

• 与密钥管理的交互作用；
• 建立密码参数与密码算法；
• 在通信实体与可信的第三方之间使用协议通信。

一般来说，数字签名管理与加密管理相类似。

4）访问控制管理

访问控制管理涉及安全参数（包括口令）的分配，或对访问控制表或权力表进行修改，也可能涉及在通信实体与其他提供访问控制服务的实体之间使用协议通信。

5）数据完整性管理

数据完整性管理可以包括以下方面：

• 与密钥管理的交互作用；
• 建立密码参数与密码算法；
• 在通信的实体间使用协议通信。

当对数据完整性使用密码技术时，其管理与加密管理相类似。

6）鉴别管理

鉴别管理包括将说明信息、口令或密钥分配给请求执行鉴别的实体，也可以包括在通信的实体与其他提供鉴别服务的实体之间使用协议通信。

7）通信业务填充管理

通信业务填充管理包括维护那些用作通信业务填充的规则。例如：

• 预定的数据率；

- 指定随机数据率；
- 指定报文特性，例如长度；
- 定期变更上述规则，例如按日、时或日历来改变这些规则。

8）路由选择控制管理

路由选择控制管理涉及确定那些按特定准则才能被认为是安全可靠或可信任的链路或子网络。

9）公证管理

公证管理可以包括以下方面：

- 分配有关公证的信息；
- 在公证方与通信的实体之间使用协议通信；
- 公证方之间的交互。

4. OSI 管理的安全管理

OSI 管理的安全管理包括对所有 OSI 管理功能的安全管理以及 OSI 管理信息的通信安全，它们是 OSI 安全的重要部分，将通过适当地选取 OSI 安全服务与机制确保 OSI 管理协议与信息获得足够的保护。例如，在管理信息库的管理实体之间的通信一般要求进行某种形式的保护。

4.5 信息安全管理的组织机构

信息安全管理的组织机构大致可以分为两类，一类是行政管理机构，它是一个战略规划、政策指导和协调类型的机构；另一类是技术服务、应急响应和技术支持类型的管理机构。

4.5.1 行政管理机构

国家层面的网络安全和信息化领导机构统一规划国家信息安全管理战略；综合协调涉及各个领域的信息化和信息安全管理工作；协调解决计算机网络与信息安全管理方面的重大问题。国家各部委和专门机构分别各司其职，其中：

- 国家密码管理委员会负责各类密码的管理工作；
- 国家保密局负责涉密网络和信息系统的管理；
- 国家安全部负责计算机网络信息安全管理中涉及国家安全的事项；
- 公安部负责维护网络公共秩序，打击利用计算机网络进行的旨在破坏社会稳定、侵犯个人和公共财产安全的犯罪；
- 工业与信息化部负责计算机网络信息安全产业管理工作；
- 教育部负责信息安全学科体系、专业和培训机构建设，以及信息安全学历和非学历人才培养。
- 国家认证认可委员会负责规划和协调全国信息安全产品和服务类型测试、评估和认证工作。

国家有关机构既有分工，又加强配合，在国家层面的网络安全和信息化领导机构的统一领导和协调下共同完成我国信息安全管理工作。

4.5.2　信息安全服务与技术管理机构

1. 国家技术标准体系的管理机构

国家技术标准体系是我国发展信息安全技术，完善自主知识产权的信息安全技术的重要法规，是从国家意志层面规范信息安全体系结构、技术要素和交流语言的通用法则。国家信息安全技术标准体系的管理机构是国家质量监督检验检疫总局，负责组织起草并颁布与信息安全有关的国家标准。在此基础上，国家和政府有关部门以及信息安全企业可进一步制定符合中国国情的法规和技术细则。

2. 信息安全测评与认证体系的管理机构

国家信息安全测评与认证体系包括对密码与非密码、涉密与非涉密的涉及机密性、完整性和可用性的各类产品及系统以及计算机病毒防范、查杀产品和系统的安全适用性与安全等级的符合度进行测试和认证。这些测试和认证工作在国家认证和认可委员会的统一协调下由分布在若干由国家或政府指定或授权的测试、评估和认证机构承担。

3. 应急响应的管理机构

应急响应体系是我国信息安全应急响应处理和技术支持的工作体系。应急响应体系保证国家基础网络设施和重要信息系统在网络恐怖活动或公共网络突发事件影响下的生存能力和快速恢复能力。国家信息安全应急管理机构包括：

- 国家信息安全应急处理协调委员会及其专职办公室，负责组织制定应急处理的方针、政策、法规和技术标准（如国家应急处理管理条例、应急服务组织的资质认证和管理条例、国家应急响应等级标准、保护目标的安全等级标准、应急处理指标体系等），培育和保持一支应急处理网络突发事件和网络恐怖活动的专业队伍，协调国家各安全主管部门处理信息安全紧急或突发事件，组织跨部门信息安全重大应急行动；
- 国家信息安全应急处理支援中心和国家应急信息交换中心，以及各行业与地区的对口应急机构，其职能包括应急信息汇集和交换、应急资源的协调与调度、保护目标的信息安全档案管理、入侵检测与系统恢复、跟踪与取证、安全预警信息分析与发布、信息安全情报协商与上报。

4. 计算机病毒防治机构

国家设立计算机病毒应急处理中心开展计算机病毒预警和防治，包括收集、解剖和分析计算机病毒信息，发现新的病毒特征并发出预警；提交病毒疫情分析报告；发布计算机病毒疫情；为受计算机病毒攻击破坏的计算机用户提供后援服务；培训计算机病毒防治的专业技术人员等。

5. 安全咨询服务管理机构

安全咨询服务指在规划、设计、实施、运行和维护直至报废的信息系统整个生命周期提供对开放互连信息系统的风险分析和安全需求分析，以及安全设计、安全检测、安全评估以及技术培训和技术支持等项业务，以保障信息系统的可信性、可靠性、可用性、可控性和可核查性。

国家各安全主管机构按照分工对提供安全咨询服务的企业按照涉密信息系统、非涉密信息系统以及涉及国家安全的专项服务分别予以资质认定和授权管理。

企事业法人单位在获得相应机构的资质审核和认定后，可从事信息安全系统集成或单项信息安全服务的安全咨询服务。

4.6 习题与思考题

1. 信息系统生命周期各阶段的主要安全管理活动有哪些？
2. 信息系统安全保护等级的划分原则是什么？
3. 阐述信息系统等级保护与分级保护的关系和区别。
4. 简述信息系统等级保护中的定级流程。
5. 使用密码技术应遵从哪些规定？
6. 一个定级为 3 级的信息系统必须具备哪些条件才能投入运行？
7. 与信息安全等级保护有关的主管机关有哪些？它们分别实施哪些监管活动？
8. OSI 安全管理涉及哪些具体的管理活动？

CHAPTER 5

第5章 信息安全管理方法与过程

5.1 信息安全管理活动概述

信息安全管理活动首先要对组织的信息系统安全进行规划，即制定信息系统安全的目标、方针和策略。这是组织的信息系统安全过程管理的纲领性指导文件，在这些文件的指导下开展一系列管理活动，包括：

- 识别和分配组织内承担信息系统安全的角色及其职责；
- 资产识别和风险管理，包括识别信息系统资产、识别并评估风险、确定安全需求、构建信息系统安全保障体系、采取基于策略的风险对抗措施等各项活动：
  - 识别信息系统资源的分布及其价值；
  - 识别信息系统资源的脆弱性或缺陷；
  - 识别信息系统资源脆弱性面临的潜在威胁；
  - 识别信息系统资源脆弱性或缺陷被成功利用的可能性及利用后对组织造成的影响或后果；
  - 识别风险分布情况及其强度（等级值）；
  - 针对风险的分布和强度确定基于策略（对抗、降低、规避或转移风险等）的安全需求对应列表，并将安全需求转换成在网络层、传输层、系统层、用户层和运行环境中具有可操作性的安全管理或安全技术措施；
  - 评估残留风险，并与可接受风险进行比较，如大于可接受风险，则应进一步采取适当的安全管理和安全技术措施将风险降低到可接受水平。
- 监管。
  - 对系统中出现的安全事件进行检测并予以处置（例如审计、告警，必要时关闭受到威胁或攻击的信息系统的部分资源或整个系统）；
  - 监控信息系统安全状态，使信息系统安全态势符合预期。

- 配置管理。
  - 选取和配置组织的信息系统的安全技术措施；
  - 按照风险控制策略配置安全设备和重要信息系统资源的运行参数。
- 变更管理。

在信息系统运行和维护阶段，当与信息系统安全有关的法律规定发生改变，组织对信息系统的功能/性能要求发生改变，信息系统自身发生改变（系统结构调整、软/硬件更新、系统升级换代等），系统运行环境发生变化，或攻防态势发生变化，都可能导致残留风险扩大，因而要重新对信息系统安全管理的各环节进行审核、调整，使信息系统的残留风险可接受。

- 制定安全事件处理策略和灾难恢复计划，并组织演练；
- 规划和制订可增强信息安全意识的培训教材和计划；
- 其他活动，包括：
  - 系统维护；
  - 安全审计；
  - 工程监理；等等。

很显然，组织的安全目标、方针和策略对于信息系统安全过程管理的指导意义在于，为有效管理组织内信息系统安全过程中的每一个环节，提出所要达到的目标、达到目标的方法和途径（即安全方针），以及达到目标所需采取的一整套规则和指令（即安全策略）。

信息系统安全目标应该反映组织的行政管理强加给信息系统的安全要求，并且遵从或考虑各种来自组织的信息系统外的约束（例如国家法律法规、技术规范、社会文化及意识形态、组织的企业文化、物理的和人文的环境等），保证在各个层次之间和各个部门之间的一致性。安全目标应该根据定期的安全性评审（如风险评估、安全有效性审核）结果以及业务目标的变化进行更新。例如某信息系统按其所属机构的国家属性，其工作业务流程和内部机构信息不得以任何形式泄露给未授权者，此即该信息系统的安全目标之一。

信息系统安全方针应该反映实现安全目标的具有可实现性的方法和途径，这些方法和途径表现为管理的和技术的形式。为实现列举的安全目标，其安全方针应当将信息系统与外部网络进行适当隔离，加强内部岗位管理，等等。

一个组织的信息安全策略由一系列具有逻辑关联性的安全规则和指令组成。这些信息安全策略必须反映组织的安全策略，并服从组织的安全策略，包括信息系统的所有者、管理者、使用者在保障信息系统安全方面的权利和义务的一致性与平衡性。按安全方针制定的信息安全策略可以是从管理上为每个岗位制定严格的操作规程，从技术上对网络隔离设备的访问控制规则进行严格配置，等等。

信息系统的安全目标、方针和策略一般使用有别于技术术语的语言（通常用一种自然的或社会化的语言）来表达或描述，但也可能采用某些数学语言以更形式化的方式来表达。这些语言表达应该清楚地说明下列关于信息系统及其资源属性和安全特性的准确含义（不造成二义性）：

- 机密性；
- 完整性；
- 可用性；
- 抗抵赖性；

- 可确认(审查)性;
- 真实性;
- 可控性;等等。

安全目标、方针和策略将帮助组织建立起信息系统的安全保护等级,设置可接受风险的阈值(等级水平)范围,明确提出组织对信息系统总的安全要求,指出达到安全要求的方法与途径,规定实现安全要求的规则与指令。

关于信息安全目标、方针和策略的进一步说明,读者可结合 5.4.2.1 节的内容深入理解。

5.2　安全管理的对象

5.2.1　资产

信息安全保护的对象也是信息安全管理的对象,是信息系统有价值的资源,即资产,这些资产概括起来包括:

- 有形(物理)资产(如计算机及其外围硬件、通信设施、建筑物、机房及内部设施等);
- 信息/数据(如文档、数据等);
- 软件(操作系统、通信协议和应用程序等);
- 信息系统直接生产的或辅助生产的产品或提供服务的能力;
- 人(管理人员、使用人员和维护人员);
- 无形资产(信誉、形象、市场份额等);等等。

识别资产并评估资产的价值是风险分析与评估的依据之一,在很多情况下需要将资产进行编组或分类。

应该考虑信息系统资产的属性,这些属性包括资产的量化价值和敏感程度,以及固有的安全特性。面临特定威胁的脆弱性将需要增强对资产的保护需求,系统运行的环境、文化背景和法律约束也可能对资产及其属性的保护产生不同影响,例如在有些环境下,个人信息的保护显得非常重要,而在另一些环境下,个人信息可能不需要保护。由此可以推断,环境、文化和法律差异对国际性组织及在跨国间使用的信息系统的安全影响的区别可能很大。

5.2.2　脆弱性

与资产相关的脆弱性包括在物理布局(含运行环境)、系统设计、施工组织与管理、运维过程管理、员工、规章制度、硬件、软件或信息中的弱点或缺陷。这些弱点或缺陷都有可能被威胁(风险主体)所开发或直接利用而损害信息系统或业务目标。脆弱性本身并不产生危害,但脆弱性是威胁对资产造成危害的条件和开发利用的对象(风险客体)。例如,缺乏访问控制机制将可能导致入侵事件,并使信息资产丢失、泄露或损毁。必须认识到,脆弱性是信息系统资产固有的,除非资产本身有所改变使脆弱性降低或消失,否则脆弱性将一直存在。在一个具体的信息系统中,不是所有的脆弱性都将被威胁利用。脆弱性如果存在对应的威胁,则必须立即识别脆弱性的存在或表现形式,并采取措施消除或降低存在的脆弱性。由于环境可能动态地变化,因此应该监视运行环境中所有的脆弱性,以便识别那些已经暴露给旧

的威胁或新的威胁的脆弱性。

脆弱性分析是对那些可以被已知的和潜在的威胁利用的弱点或缺陷进行测试和评估，在分析过程中必须考虑运行环境和现有的安全措施对分析结果的影响。

脆弱性的测评结果可以用较粗粒度的等级(例如高、中和低)或更细粒度的等级来表示其严重程度的差异。

5.2.3 威胁

此处的威胁是指开发、利用信息系统资源(产)的脆弱性或缺陷，以渗透、入侵和攻击等方式对某一、某些信息资产或整个系统的机密性、完整性和可用性等进行破坏的企图或可能性。

威胁具有潜在破坏力。威胁所产生的损害来源于内部或外部威胁主体对(正在被信息系统或服务处理的或存储的)信息或系统组件的直接或间接攻击，例如对信息的未经授权泄漏、修改、讹用以及使其不可用或者丢失。威胁利用资产存在的脆弱性损害资产。威胁可以是自然或人为的，也可以是存在于内部或外部的，并且可能是偶然或蓄意存在的，各种形式的威胁都要识别出来并对其危害等级和可能性作出评估。

表 5.1 所示为一些常见的威胁示例。

表 5.1 常见威胁示例

人为威胁		自然威胁
蓄意的	偶然的	
偷听 信息修改 系统劫持 恶意代码 偷窃 暴力攻击等	错误和遗漏 文件删除 不正确的路由 物理事故等	地震 雷电 洪灾 火灾等

5.2.4 影响

当威胁成功实施后，无论损失大小均被称为安全事件或事件。事件的直接结果可能是破坏某些资产，毁坏信息系统，以及丧失机密性、完整性、可用性、抗抵赖性、可确认性和可靠性等。可能的间接影响包括财产流失，市场份额丢失或公司形象损坏。影响(Impact)是指威胁成功实施后对信息系统或其资源所造成的(以有形和无形的、货币化和非货币化的方式计算的)结果。安全事件发生的频度也是评估影响的重要参数，特别是在单个事件引起的危害较低，但多个事件所累积的危害很大时，需要考虑事件的发生频度。对影响的评估是风险评估和安全措施选择的重要基础性工作。

有很多方法可用来对影响进行定性和定量的度量，例如：

- 财务成本核算；
- 对其严重程度设定一个经验性的数值标度，如 1～10；
- 使用预定义的表示影响程度的形容词来度量影响的程度，如低、中、高。

5.2.5　风险

风险用来描述信息系统资产的脆弱性，针对这些脆弱性的威胁企图、威胁成功的可能性（概率），以及由此造成的影响等要素的递推关系，风险通过评估威胁利用资产的脆弱性对组织的信息系统造成危害的可能性及危害的后果来度量。

一个威胁或多个威胁可以利用一个或多个脆弱性，虽有某些对应关系，但一般并无固定的对应关系。风险用两种因素的组合来度量，即安全事件发生的可能性及安全事件发生后造成的影响。资产、脆弱性、威胁和安全保护措施等方面的任何变动都可以对风险的分布情况和风险强度（值）产生影响。及时地检测或识别环境或系统的变动能增加识别风险的机会，以便采取措施减少风险。

5.2.6　残留风险

通常，采取将管理和技术相结合的安全保护措施后，风险可以被降低、规避或转移。如果要对抗更多的风险，就需要更多的安全资源开销。实际上，信息系统不可能是零风险，都会存在残留风险，但残留风险必须对保证信息系统业务的持续服务能力来说是可以容忍的，即通常说的可接受。因此信息系统安全的方法并不在于追求零风险，而在于获得适度的安全保护水平，或将风险降低到可接受程度。判断现有的安全保护措施是否有效和充分的依据的就是残留风险是否可以接受。

信息系统的安全管理机构应该意识到所有残留风险可能带来的影响以及发生安全事件的可能性。是否接受残留风险是由安全管理机构及其负责人决定的，他（们）将承担由于安全事件发生所造成后果的责任。当信息系统不能接受残留风险时，安全管理机构及其负责人应该授权实施附加的安全保护措施或调整安全策略，以降低残留风险到可接受的水平。

5.2.7　安全措施

安全措施是保障信息安全的技术和管理的实践、过程或者机制的通称，用来消除或减少脆弱性，对抗威胁，限制安全事件的发生和影响，检测安全事件和促进恢复活动。有效的安全保护体系通常需要综合使用多种不同的安全措施，为信息系统资产提供必要而充分的一层或多层安全保护服务。

安全措施对于信息系统安全保障的作用和功能在于：

- 消除或减少信息系统资产的脆弱性；
- 防范不期望事件或行为的发生；
- 威慑蓄意或敌意的入侵、攻击和破坏企图；
- 检测入侵和攻击行为、事件并发出预警和告警；
- 限制不期望事件的扩大和不良影响；
- 修正/校正/增强已有安全措施，使之满足安全要求；
- 恢复设备或系统的正常运行能力；
- 监视信息系统关键业务设施的安全运行状态。

选择合适的安全措施对于正确地实现安全解决方案是极为重要的。

5.2.8 约束

约束通常由组织的管理者根据国家法律和系统的具体情况设定，并且受组织外的因素和信息系统运行环境的影响。常见的约束如下：

- 组织的结构与机构；
- 业务运行流程；
- 财务计划及执行；
- 运行环境；
- 员工素质；
- 时间段或周期；
- 法律规定及强制性制度；
- 技术规范和标准；
- 文化/社会背景及和谐程度。

当选择并实现安全措施时应考虑进行以下活动：定期复核现有的或新的约束，并识别约束的变更。约束可能随着时间、地理位置、社会环境和组织文化的变化而变化。信息系统运行的环境和企业文化将对一些安全要素（特别是威胁、风险和安全措施）产生影响或重大影响。

5.3 安全管理模型

信息安全管理有多种模型或模式，各种模型都是从不同角度构建的，都有各自特别适用的范围或对象，但各种模型所提出的安全管理概念都有利于对信息安全管理的原理和实践进行理解。归纳起来，目前较为流行的模型有以下几种：

- 安全要素关系模型；
- 风险要素关系模型；
- 基于过程的风险管理模型；
- PDCA（Plan-Do-Check-Act）模型。

上述概念模型和组织的业务目标一起可形成一个对组织的信息安全目标、方针和策略的安全管理轮廓。信息安全的整体目标就是保证组织的信息系统能够安全地运行，并且将风险控制在可以接受的程度。任何安全措施都不是万能的，也不是对任何风险都是完全有效的，因此需要规划和实施预防意外事件的数据备份或系统备份，以及事件发生后的恢复计划，构建可将损坏程度限制在一定范围的安全保障体系。

5.3.1 安全要素关系模型

信息系统安全是一个需要从不同方面来观察和研究的多维问题。为了确定和实现一个全局的、一致的信息安全方针和策略，一个组织应该考虑与之相关的所有方面的问题。图 5.1 说明了资产可能受到大量潜在威胁的情况。一般来说，这些威胁的集合总是随时间变化的，并且只有部分是已知的或可以预见的。

这一模型表示的含义如下：

- 环境、约束和威胁，其中环境情况和约束条件是相对稳定的，并且其变化是可以预见

的，威胁则是动态变化的，并且只有部分是已知的或可以预见的；

- 应予保护的组织的信息系统资产及其价值；
- 这些资产存在的脆弱性；
- 为保护资产、消除或减少脆弱性、降低风险所选择的安全保护措施；
- 评估可接受的残留风险。

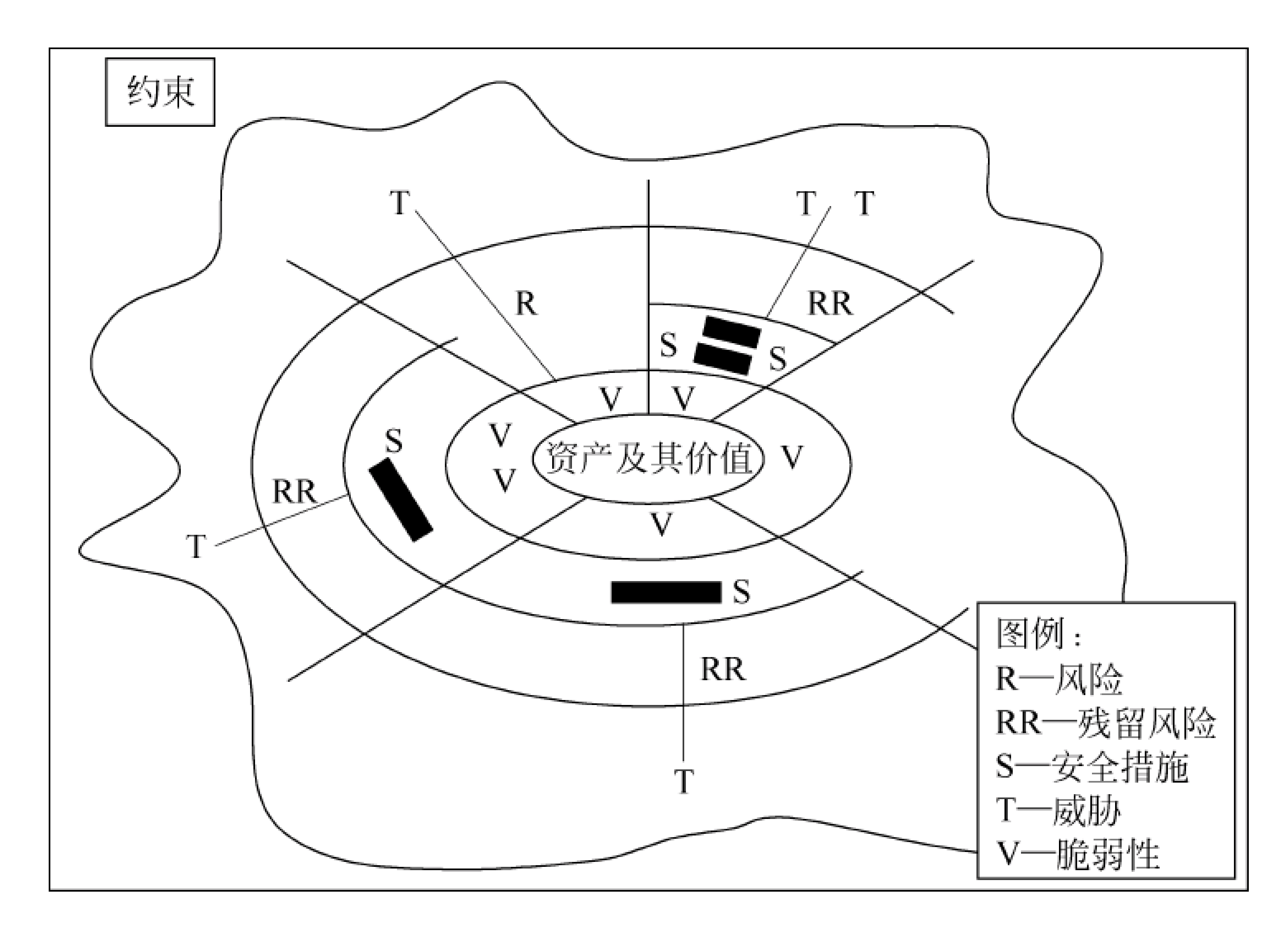


图 5.1　安全要素之间的关系

如图 5.1 所示，一些安全措施(S)可以在降低与多种威胁(T)和多种脆弱性(V)相关联的风险(R)中起作用。有时需要几种安全措施才能保证残留风险(RR)是可接受的。在残留风险经过评估并认为是可接受的情况下，即使出现威胁，也无必要采取额外安全措施，但应加强监视；在另外一些情况下可能存在某种脆弱性，但没有已知的威胁利用它，可以采用一些安全措施来监视威胁实施的环境，以确保没有威胁能开发或利用该脆弱性。模型中的约束(C)可以影响安全措施的选择。

这一概念模型展示了需保护的信息系统资产及其价值、脆弱性、威胁、风险、残留风险，以及环境和约束等安全要素之间的关系，提供了一种围绕资产及其价值进行安全管理的思路。

5.3.2　风险要素关系模型

图 5.2 阐述了与风险相关的安全要素之间的关系。为了简单、清晰起见，这里只表示了主要关系。

信息系统的资产可能存在风险，例如信息的未授权泄漏、修改、不可用和抵赖，信息服务的不可用或能力降低等。对于这些风险，首先要识别出资产真实的价值，然后要考虑哪些威胁可能会造成影响，进一步，反过来考察哪些脆弱性可能会被这些威胁利用，造成影响，以及它们发生的可能性有多大。根据资产的价值、脆弱性的严重程度以及威胁的等级确定出风险大小。对风险的识别和度量能够导出整个安全保护需求，并通过安全措施的实现来满足。安全措施的实施可以对抗威胁，并减少风险。

这一概念模型从风险要素之间的逻辑关系方面提供了围绕风险要素进行安全管理的思

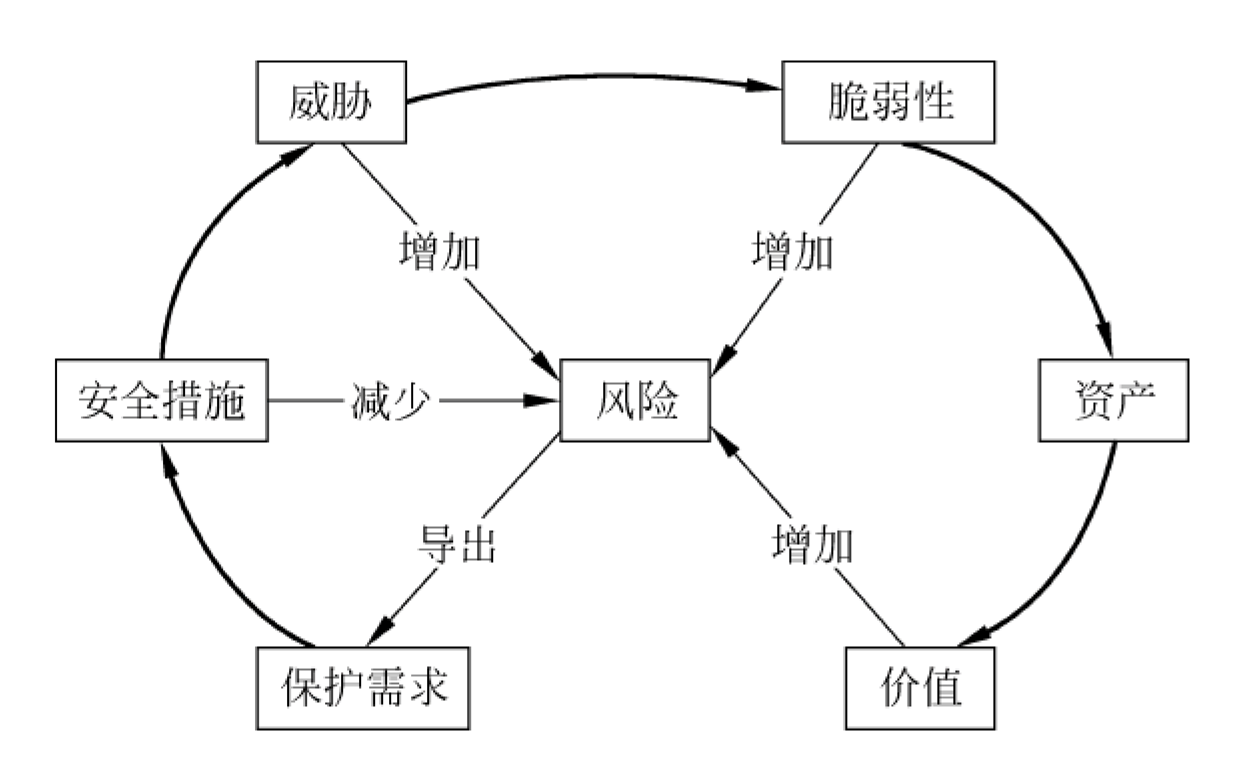


图 5.2　风险要素关系模型

路。这一模型与图 5.1 所示的模型比较，在风险控制成本与被保护的资产价值之间考虑了平衡。

图 5.3 和图 5.4 分别说明了资产、保护需求和威胁、脆弱性之间的逻辑关系。

图 5.3 说明保护需求源于资产及其价值，重点考虑了威胁利用脆弱性对资产构成的风险情况，三者之间建立了在考虑威胁因素情况下关于保护成本与资产价值的平衡关系。

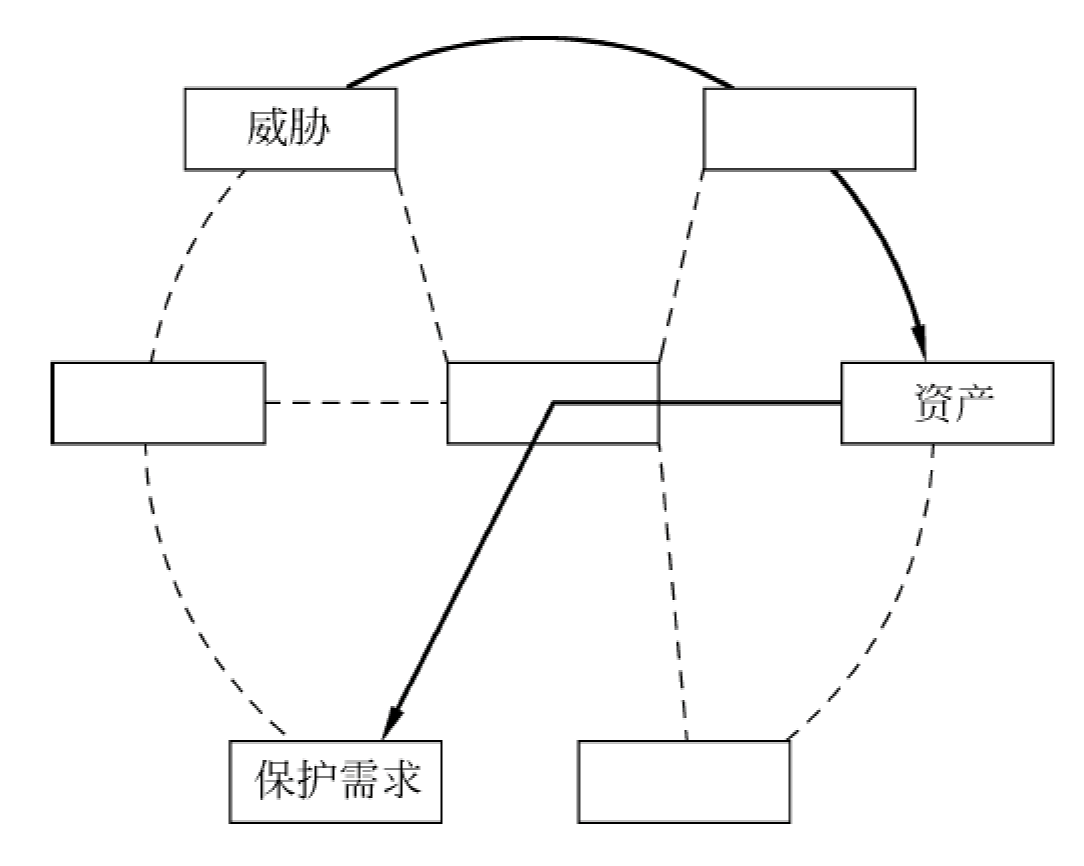


图 5.3　资产与保护需求的关系示意

图 5.4 说明保护需求源于资产及其价值，重点考虑了由于资产脆弱性引起的风险情况，三者之间建立了在考虑资产脆弱性情况下关于保护成本与资产价值的平衡关系。

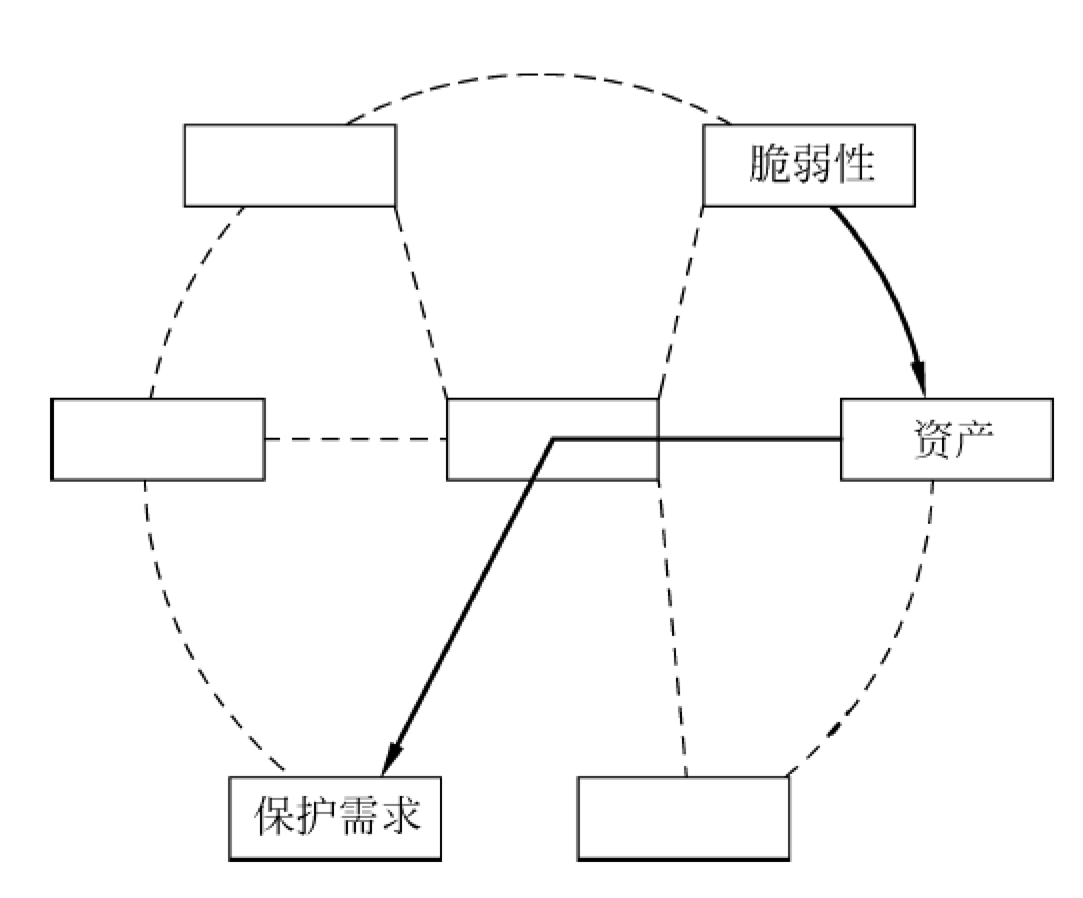


图 5.4　资产脆弱性、资产价值和保护需求的关系示意

5.3.3　基于过程的风险管理模型

基于过程的风险管理是一个由许多子过程组成的系统工程。其中一些过程，例如配置管理和变更管理，可以用来控制安全以外的其他过程。经验表明，过程风险管理及其风险分析子过程在信息安全管理中极其有用。图 5.5 说明了基于过程的风险管理的几个方面，包括风险分析、变更管理、配置管理和风险调控等。

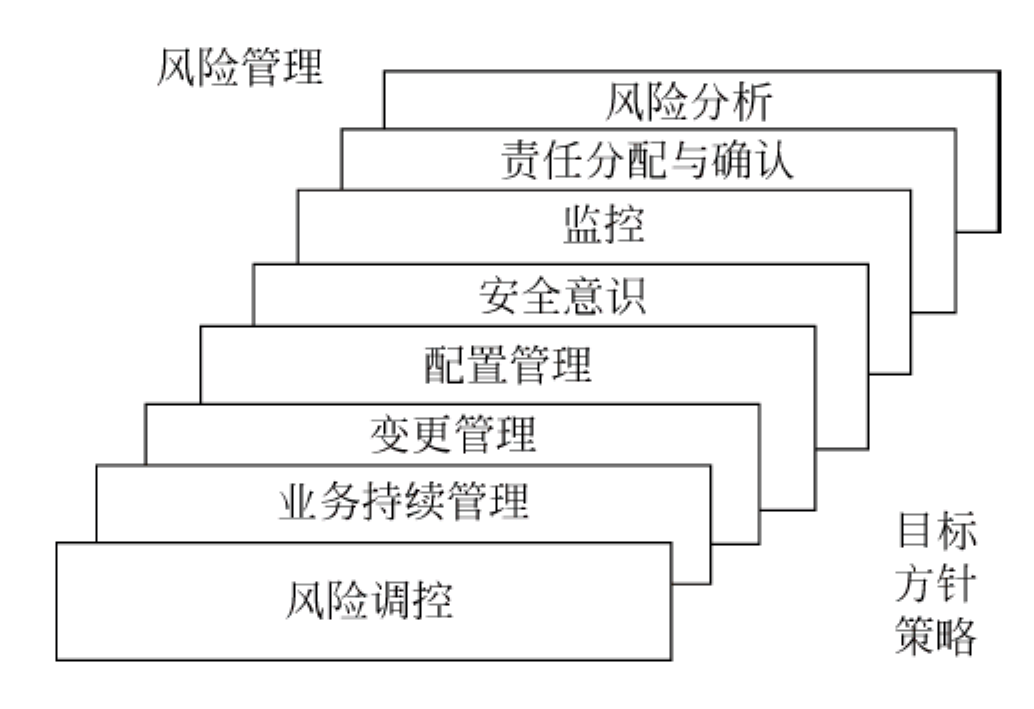


图 5.5　基于过程的风险管理

风险管理是一个基于可接受成本的、对影响信息系统安全的风险进行识别、控制、最小化或消除的过程。风险管理根据评估的风险与保护效能和保护成本的比较，综合考虑不同类型的安全措施及配置这些措施所花费的代价以及从保护中获得的利益之间的平衡关系，然后制定出与组织的信息安全策略和业务目标相一致的信息系统安全方针和实现策略。安全措施的选择与风险有关。可接受的残留风险的等级是风险评估的基础。重要的是，要在识别和实现安全措施过程中对所耗费的最小成本和组织所拥有的资源价值之间取得平衡，也就是说信息系统的安全保护要适度。

风险管理是一系列渐进的活动。对于新系统或者计划阶段中的系统来说，要准备将风险管理贯穿到设计、开发和系统运维过程中。对于已经存在的系统，应该适时引入风险管理。而当计划对系统进行重大变更时，风险管理应该成为这一变更计划的一部分。风险管理应该考虑一个组织中的所有信息处理系统，而不应该孤立地应用到某一个系统。同时特别强调，安全措施本身也可能包含脆弱性，进而可能导致新的风险。因此在设计或选取安全保护措施时，要注意不因采取新的安全措施而引入新的安全脆弱性，从而导致新的风险，故选择安全措施必须小心，要做到在减少风险的同时，不引进新风险。

风险分析是对那些需要被控制或被接受的风险进行识别。信息系统的风险分析涉及对资产价值、脆弱性和威胁以及威胁的后果进行综合分析。风险是通过对机密性、完整性、可用性、可靠性、抗抵赖及可确认性的可能损坏进行识别和分析的。

责任分配与确认是风险管理中的一种重要的措施，它明确无误地将责任进行分配并确定责任者。责任需要被分配给信息系统的资产所有者、管理者、供应商和使用者，并能在需要时予以确认。因此，资产的所有权和相关的安全责任人加上对安全行为的审计，可以回溯并追究安全事件的责任，以此增强相关人员的安全意识，并对来自内部或外部的恶意行为人构成威慑，这对信息系统的安全来说非常重要。

监控是实施安全措施所需要的，安全措施本身的监控功能则能确保安全功能正常发挥作用。在安全设备运行期间，当环境改变后，监控功能应仍能维持所设计的效能。系统日志的自动审核和分析是帮助系统性能达到预期效果的有效工具。这些工具也可以用来检测有害事件，并可以对某些潜在威胁起到威慑的作用。

需要定期验证安全措施是否保持设计的效能。通过监控和对安全效能符合性的检测可以确定安全措施正常发挥功效。很多安全措施会产生输出，例如日志、报警信息等。通过检查这些输出信息可以发现安全事件和分析潜在的安全事件。系统审计功能可以在安全管理方面提供有用的信息，并能提供监控所需的输入信息。

安全意识是确保信息系统安全所需的基本要素。组织中的有关人员缺乏安全意识以及不规范或不良的操作习惯会极大地降低安全措施的有效性或者引发风险。一个组织中的操作人员通常被认为是信息安全链中的薄弱环节之一。为确保组织中的每个人都有足够的安全意识，非常有必要建立和维持有效的安全意识培训规程。建立这个规程的主要目的是向组织的员工、合作伙伴、供应商阐明：

- 安全目标、安全方针和策略；
- 与他们的角色和责任相关的操作规范要求；
- 从职业道德和行政、技术规范上需要养成的良好习惯和必须遵从的行为准则。

此外，安全培训规程还应提供规范员工、合作伙伴和供应商在安全保障体系中承担的安全责任和义务的内容。

应使组织内从高层管理人员到负责日常事务的员工都知晓并贯彻实施安全意识规程。通常需要针对组织中不同部门的人、不同的角色以及负不同责任的人制作相应的安全意识教育材料。一个比较合理的综合性的安全意识规程培训是分阶段完成的。每个阶段的培训内容都以以前的经验为基础，从安全的概念开始到如何解决操作与监控中出现的安全问题。

组织内的安全意识教育规程可以包括各种各样的活动，其中一个活动是安全意识教育材料的制作和发布。另一个活动是举办训练课程，对所有员工有针对性地进行合适的安全技术和实践培训。此外，训练课程还应提供若干特定安全专题方面的具有专业水准的讲座教育。一般来说，在业务培训计划中加入安全知识是行之有效的。对于安全意识培训规程的制定需要考虑以下几个问题：

- 培训需求分析；
- 培训规程的开发与提交；
- 对培训规程执行情况的监控；
- 安全意识培训规程的内容。

配置管理或控制是启动并维持系统参数配置的过程，以正式或非正式的方式完成。配置管理的基本安全目标是确保及时获得信息系统变更后所需的安全运行参数和安全控制参数配置表，以不降低安全措施效能和组织的整体安全的方式对已批准的系统变更进行安全管理。

变更管理是另外一种过程，当一个信息系统发生变更时用来帮助识别新的安全管理需求。信息系统及其运行环境经常发生变化，这些变化或者是由新的信息系统特性和服务所导致，或是因为发现新的脆弱性和威胁。信息系统的变更包括以下内容：

- 运行环境；
- 新的程序；
- 新的功能和性能；
- 软件升级；
- 硬件更换；
- 新增加用户，包括外部用户组或匿名组；
- 增加子网和与外部网络互联；
- 新的脆弱性或威胁出现。

当信息系统发生变动或者计划变动信息系统时，重要的是要确定这些变动会对系统的安全带来的影响。如果系统拥有配置控制中心或者其他组织机构来管理系统的技术变动，那么应指定信息系统安全官员并赋予相应的职责，以便对这些变动是否会影响系统的安全以及影响的程度做出判断。在某些情况下，需要对变动可能降低系统安全的原因进行分析。这时往往需要评估安全性降低的程度，并基于所有有关的事实做出管理决策。换句话说，改变一个系统需要适时地考虑对安全的影响。对于涉及购买新的硬件、软件或服务的重大改变，需要分析以确定新的安全需求。另一方面，许多变动只造成小的系统性能变化，不需要像发生结构性变动那样做深入的分析。然而不管系统变动大或小，都需要进行风险评估，确定保护的收益与保护的成本之间的平衡。

业务持续性管理是维持业务不间断的管理过程。业务持续性管理为确保业务的连续运营提供进程和资源的持续可用性。业务持续性管理还包括应急计划和灾难恢复。

应急计划是当信息系统运行和维持能力降低或系统不可用时如何维持或快速恢复基本运行业务的保证。这些计划应该涉及各种可能的情况，包括：

- 规定各种业务容忍中断的时间，通常以小时或分钟数计算；
- 预估不同类型设施所受的损失；
- 估计建筑物及其附属设施所受的总损失；
- 恢复到损坏发生前状态所需的时间。

灾难恢复计划描述怎样使受安全事件影响的信息系统恢复运行。灾难恢复计划包括：

- 制订灾难的识别准则；
- 确定各种恢复活动的职责；
- 履行恢复计划的职责；
- 恢复活动的过程描述；
- 测试恢复计划是否有效。

风险调控过程贯穿于安全工程的整个生命周期，图 5.6 说明了风险调控的各个环节及其调控流程。

这一模型的优点是强调了基于风险调控的各个阶段，具有一定的可操作性，缺点是对于各个阶段之间的关系没有给出具有逻辑性的描述。

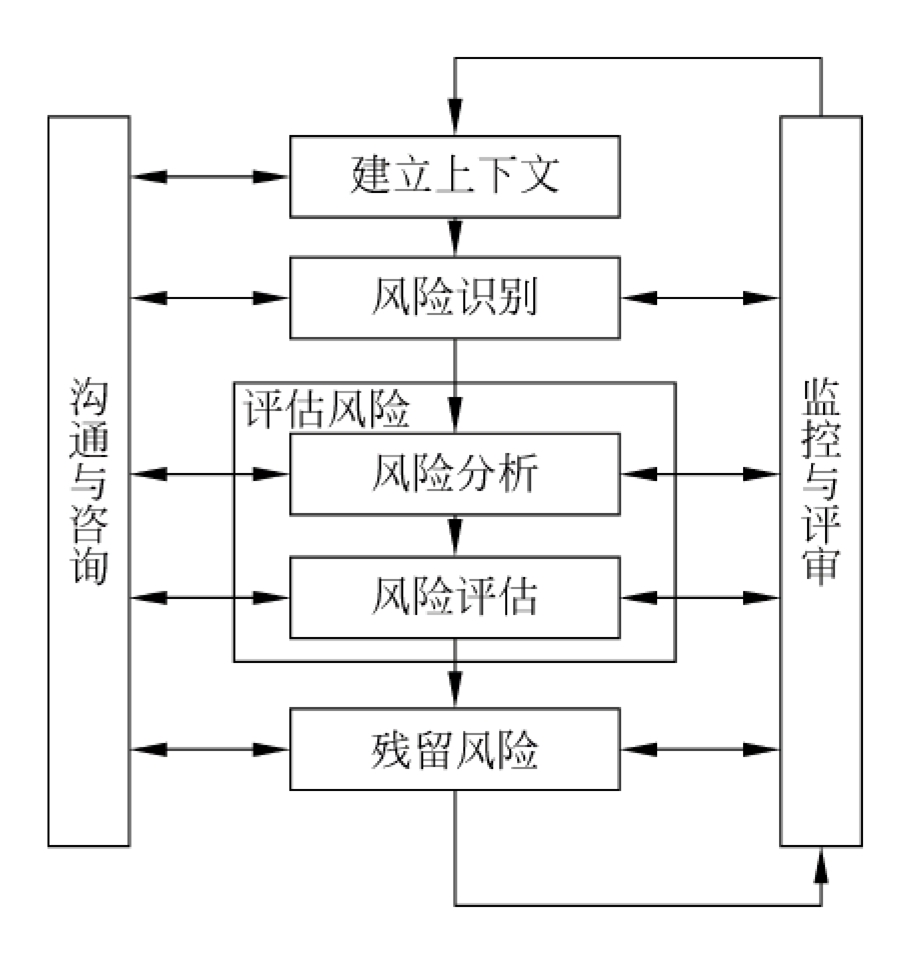


图 5.6 风险调控过程概览

5.3.4 PDCA 模型

PDCA(规划—实施—检测—改进)模型如图 5.7 所示。

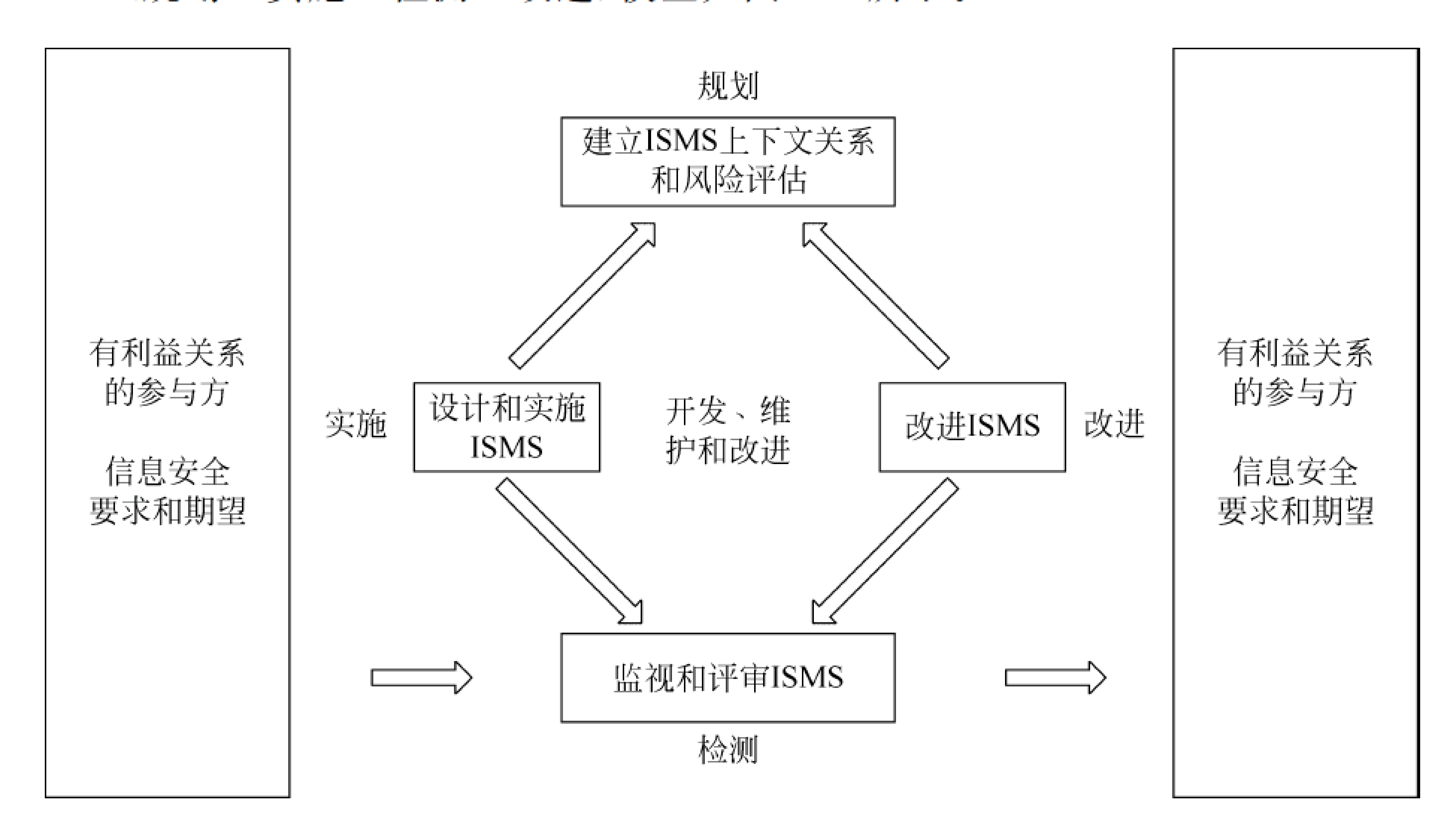


图 5.7 PDCA 过程模型

1. 规划(Plan)——对组织的信息安全进行总体规划

建立 ISMS(Information Security Management System,信息安全管理体系)的结构关系;提出信息安全的目标、方针和策略,其中,安全目标是一个满足组织对信息系统安全要求的指标体系,安全方针是达到安全目标的方法和途径,安全策略是实现安全目标的一系列规则和指令。

2. 实施(Do)——设计和实现

对实现信息安全目标所需的过程程序进行设计和工程实现。

3. 检测(Check)——监控和审核

采用自动工具和人工检测结合的方法,根据安全目标、方针、策略和运行实践情况对过程程序的安全性能进行检测和审核,并给出与安全要求指标是否符合的定量或定性的结论。

4. 改进(Act)——改善

改善或改进过程程序的安全性能,使之符合安全规划中提出的安全要求指标。

表 5.2 所示的 6 个步骤能够帮助用户建立一个信息安全管理体系(ISMS)。

表 5.2 建立信息安全管理体系的步骤

第一步	第二步	第三步	第四步	第五步	第六步
制定信息安全管理策略	确定管理的范围 信息资产	风险评估 脆弱性 威胁 影响	风险管理 组织的风险管理方法	选择安全措施(控制目标和要执行的控件) 控制目标和控件 附加的控件	准备可用性说明

第一步 制定信息安全管理策略

考虑所有信息资产以及它们对组织的价值,然后设置一个可以用来识别信息重要程度

以及理由的策略。从实践的观点来看，只有那些具有重要价值的信息才需要得到关注。

第二步　确定管理的范围

排除低价值的信息，确定整个组织所关心的信息种类或信息体。在这种情况下，需要考虑所有的信息系统资源和它的外部接口资源以及通信过程、文件柜（文件）、电话交流（语音信息）、公共关系等范围之内的信息。

第三步　风险评估

判断资产损失的风险，要考虑影响风险的方方面面。对于极端情况，还要考虑技术的复杂性，考虑开发新技术和业务的成本，以及工业间谍活动和信息战等方面对风险评估的影响。

第四步　风险管理

对各类风险进行管理，包括对技术、人员、管理程序和物理方面的因素以及保险契约等的风险管理。风险一旦发生，需要想办法抑制或减小危害，更需要一个有效的可持续计划。

第五步　选择安全措施

按安全需求选择安全措施，其中包括选择合适的风险管理措施。

第六步　准备可用性说明

证实所选择的所有安全措施的充分性，并证明它们的必要性，进一步说明没有被选中的安全措施是与本项不相关的。

这一模型从安全工程实施的过程角度提供了安全管理的思路，考虑了与信息安全管理有关的诸多方面，也具有一定的可操作性，但对风险管理的对象及风险管理的方法描述有些模糊，因此很难适用于对开放互连信息系统的安全管理，但更适合于对软件系统开发过程中的安全管理。

本节提到的几种信息安全管理模型都是从不同角度或根据不同应用领域的需要设计的，都有一定的参考价值，对于理解和认识信息安全管理可以起到“敲门砖”的作用。在面对具体的信息安全管理问题时，建议读者不要盲目套用，而应自己运用信息安全管理理论和方法论设计符合实际需要的信息安全管理模型。

5.4　信息系统生命周期的安全管理

本节从两方面介绍信息系统生命周期的安全管理，一是安排和规划信息安全管理，二是信息安全管理技术。

对信息安全管理进行安排和规划涉及与组织的信息系统安全有关的管理人员及其职责。

信息安全管理技术描述在信息系统生命周期里与管理有关的活动（例如规划、设计、实施、测试、部署或操作等）中涉及的那些知识技能和操作技巧。

5.4.1　安排和规划

本部分涉及信息安全管理的各种安排和规划活动的内容。它关系到信息系统的规划、建设、运行、维护过程中管理者的职责等，同时也关系到那些对信息系统的实际应用活动负责的管理者。总之，这一部分的内容包含了对一个组织的信息系统有管理职责的人都有用

的信息。

现在,政府和商业机构越来越依赖信息系统来指导和完成业务活动和与公众、社会的信息交互。信息和信息服务的机密性、完整性、可用性、抗抵赖性和可靠性的丢失会给组织带来不利影响,因此需要保护信息系统的信息和信息服务,提高相应的安全管理水平。在开放系统互连网络环境下的信息系统,由于组织内外的网络是连通的,这种保护需求越来越迫切。

信息安全管理是一个获得信息系统及其资源的机密性、完整性、可用性、抗抵赖性和可靠性,并将其维持在一个合适的水平的过程。

为了履行对信息系统安全的管理责任,安全管理活动必须作为组织的管理计划中不可缺少的组成部分贯穿于组织的管理过程中。因此,在这里并不拓宽管理的一般含义,而更注重于安全方面的管理与一般管理的联系。

图 5.8 从安排和规划的角度描绘了安全管理过程的主要阶段和活动。

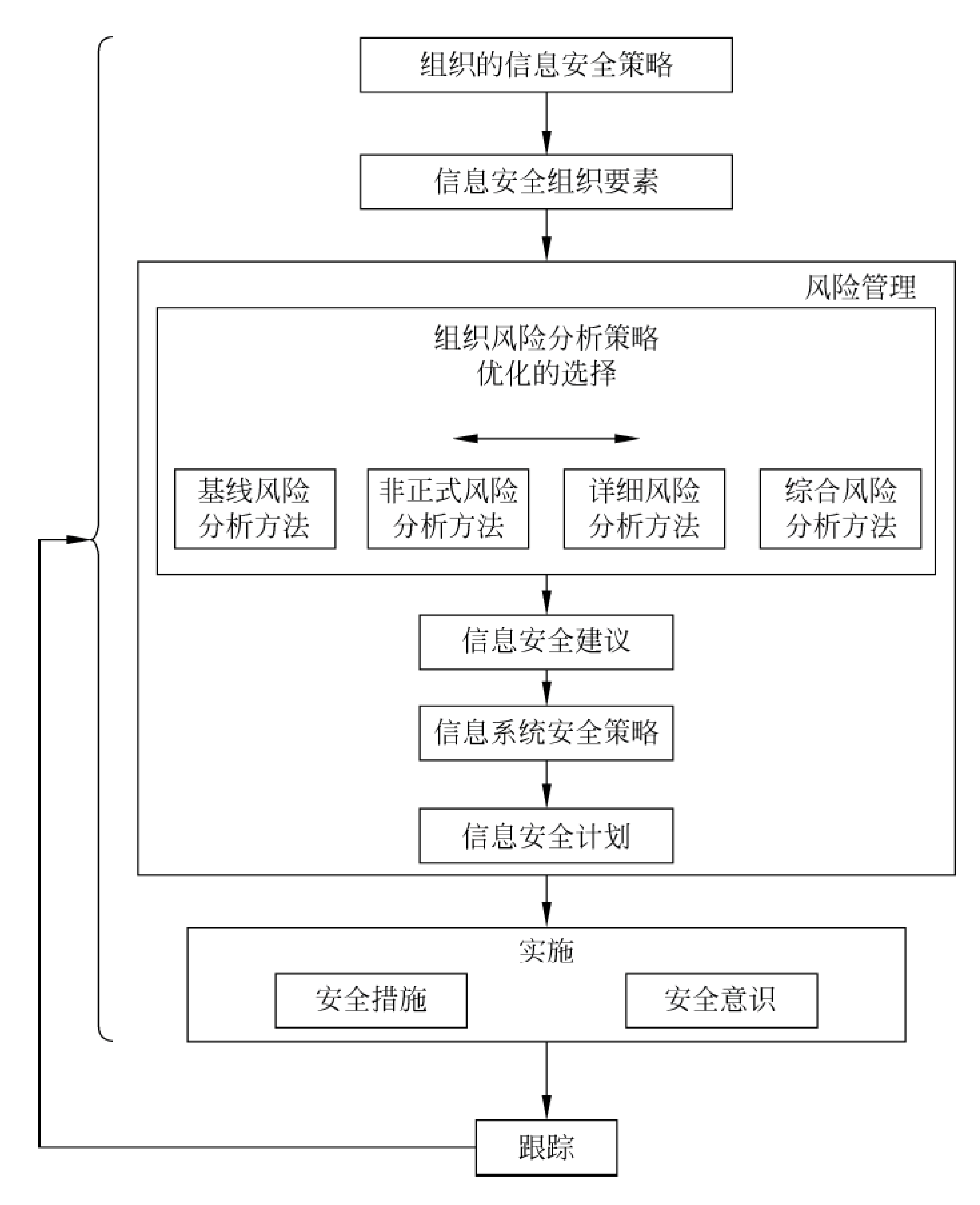


图 5.8 安全管理过程

组织的信息安全保护的出发点是保护业务目标的实现,然而为了实现这一业务目标需要制定信息安全策略。因此,安全策略只有作为管理体系结构的一部分,其既定的安全目标才能得以实现,故图 5.8 标识的所有活动和功能都很重要。

图 5.8 所描述的安全管理过程大致分为 5 个部分,即组织的信息安全策略、信息安全的

组织要素、风险管理、实施以及后续的跟踪活动(维护、监控、检查、培训、评审等)。

5.4.1.1　组织的安全策略和信息安全策略

1. 组织与信息安全策略

组织的安全策略一般应该包括组织的技术策略和管理策略,作为阐述组织信息系统安全策略的指导性文件。信息系统安全策略的陈述应该使用简明的、有说服力的语言来阐明信息安全的重要性,特别是当信息安全必须依从于某个具体策略时尤其如此。一般来说,组织的信息安全策略应服从组织的安全策略、技术策略和业务策略等,而组织的下属部门信息安全策略应服从信息系统安全策略,以此类推。一个组织无论采用什么样的组织结构和使用什么格式的文档,重要的是保持对安全策略有关的表述之间的一致性,避免部门之间有关安全策略表述的二义性或冲突。

2. 组织的信息安全策略要点

信息安全策略至少应包括以下要点:

- 信息安全需求,例如机密性、完整性、可用性、抗抵赖性和可靠性等需求,尤其是要尊重资产所有者安全需求的意愿;
- 组织的基本结构和信息安全责任分配;
- 信息安全保护等级的定义规程;
- 员工选聘、上岗、在岗、下岗、解聘或辞退的规范;
- 与安全意识有关的职业道德和业务素质的培训和教育规程;
- 法律的和管理的责任;
- 外购外包管理规范;
- 风险管理规程;
- 应急和恢复计划;
- 安全事件处理规范和实施计划。

5.4.1.2　信息安全的组织结构

1. 角色和责任

信息安全与组织内信息系统的所有者、管理者和使用者都有关。安全责任的指定和划分应该保证高效地完成所有的信息业务。不管组织的规模、结构和管理体系,也无论实现信息安全目标的方式,都应配备信息安全管理委员会,用于解决组织内跨部门和跨技术学科的协调问题,制定或批准信息安全策略,颁发安全管理指南和技术规范;并且配备信息安全官员,即一个组织内信息安全各个方面的组织者和指挥者(实际上是组织内部所有信息安全方面的权威管理人员)。

同时应该对信息安全管理委员会和信息安全官员角色两者进行良好的定义和责任划分,以确保在执行组织的信息安全策略时有充分的人力、资金、资源保证及权威性。

1) 信息安全管理委员会

信息安全管理委员会中应包括具有识别信息安全目标、确定信息安全方针和策略、解释信息安全策略、草拟信息安全规程、评估信息安全有效性,以及指导信息安全官员等所必需的权力、知识和技能的专家。委员会充当的角色如下:

- 向信息系统管理机构提供关于信息安全战略规划方面的建议;

- 审核本组织的信息安全策略，并获得信息系统管理机构的正式批准；
- 监督信息安全管理活动；
- 评审组织的信息安全策略的有效性；
- 审议信息安全管理的重大变动行动；
- 对规划过程和信息安全活动的实现中所需要的资源（人力、财力等）配置提出建议。

为使信息安全管理委员会具有效力，委员会还应该包括具备信息系统技术知识背景的成员，以及主要的信息系统供应商和使用者代表，因为开发一个实用的信息安全策略需要这些领域的知识和技能。

2）信息安全官员

由于信息安全的责任较为分散，可能存在一种风险，即最后可能没有人对整个系统或子系统的安全负责任（即没有人对全局或局部安全负责）。为了避免此类问题，应将责任分解后指定给具体的人。建议设立一个专门的岗位——信息安全官员，作为一个组织内信息安全各个方面的核心人物，应选择一个具有安全和信息技术背景的人担任。其主要职责如下：

- 组织和协调与信息系统安全有关的规章制度和操作规范的起草；
- 从细节上具体管理信息安全活动；
- 适时地向信息安全管理委员会和组织的安全主管官员报告信息系统的安全状况；
- 牵头事件调查并起草处理意见；
- 管理全组织范围的信息安全意识教育项目；
- 为信息系统工程和系统管理员以及下属部门的信息安全官员分派指定的安全事项。

2. 主动支持

有效的信息安全活动需要得到各个层次管理人员的支持。这些支持包括：

- 帮助理解组织的全局业务需求；
- 帮助理解组织内的信息安全需求；
- 利用示范方式推动信息安全意识的教育培训；
- 无保留地陈述信息安全需求；
- 愿意将行政或技术资源调配给信息安全活动；
- 组织的最高领导层清楚地意识到信息安全的含义、范围和程度。

信息安全的目标应该通告给整个组织的每一个员工或者合作者，让他们都清楚地知道自己的角色和安全职责、对信息系统安全的作用，以及自己的权利和义务。

3. 协调一致

应对所有的设计、开发、维护以及运行活动进行协调，确保将信息安全保护措施贯穿到信息和信息系统的整个生命周期。信息系统所属组织的结构必须适应与信息安全有关的协调活动，这就需要得到各个管理层在规范和标准方面一致的支持。这些规范和标准可能是行政性的和技术性的，包括国际的、国家的、行业的、地方的、区域性的以及组织自己的，这需要在国家法律约束下根据组织的信息安全需求进行选择和应用。

使用规范和标准的好处在于：

- 信息系统安全符合国家整体安排，具有合法性；
- 信息系统可获得综合性的、完整的安全体系性保障；

- 组织内的各信息系统间和与组织外的信息系统之间具有互操作性；
- 信息系统内各子系统之间在安全和效率之间获得平衡；
- 安全保障方法具有可移植性；
- 系统规模变动时具有兼容性和经济可行性。

5.4.1.3 风险管控策略和关键问题

1. 风险管控的策略

任何组织的信息安全需求都与在业务运行规模、方式及其环境和文化背景下可能招致的风险紧密相关。风险管控策略的选取必须考虑与这些因素的关系。

有时候，一个组织可能决定暂不或暂缓执行某些安全保护措施，这种情况只能出现在该组织的基于风险管理的信息安全策略已获得高层审核并获通过之后。在做出这样的决定之前要意识到风险可能产生的不利影响，以及突发事件发生的可能后果。只有在慎重考虑可能出现的种种不利影响之后才能做出不保护或者缓保护某些资产的决定。

在开始进行风险分析活动前，应该以文档说明方式确定风险分析的方针，即确定选择风险分析方法的准则，保证选择的风险分析方法适合信息系统的运行环境和实际需要，能够将安全资源相对集中到需要重点保护的地方，同时兼顾信息系统的整体安全平衡。

各种风险分析方法的基本区别在于风险分析的深度和细微程度方面。对所有的信息系统都做详细风险分析会造成某些组织不堪重负的太大花销；另一方面，对重要风险只给予一般的关注也是不合适的，所以需要根据信息系统存在的实际的风险分布及其强度情况在各种选择间进行平衡。关于具体的风险分析方法将在 5.4.2.2 节详细描述。

2. 风险管控的关键问题

无论采用哪一种风险分析方法，其目的都在于准确地识别系统风险的分布及强度，以此确定安全需求，选取有针对性的安全措施将风险控制到一个可接受的水平。其中，如何选取安全措施、如何研判残留风险是可以接受的是风险管控中的关键问题。对此，提出以下建议：

1）安全措施的选择

可以选择的安全措施分为两大类：一是可以预防、监视和检测安全事件发生和降低安全风险的与管理、技术有关的行为和设备或组件；二是可以从安全事件中将信息系统进行快速恢复的技术设备或设施。

在选择满足安全需求的信息安全设备时应遵从公通字[2007]43 号文件《信息安全等级保护管理办法》中关于信息安全设备的测评和认证规定。

选择的安全措施一般应协调发挥作用而不强调相互独立地运行，以便在有条件的地方实现安全控制信息的共享，尽可能实现安全控制的联动。

在选择安全措施时尤其要注意不能留下安全间隙或空白。这些安全间隙或空白可能给各种威胁行为绕过或穿透已有的安全措施实施攻击提供通道。

对新的信息系统或发生重大变动的信息系统而言，安全措施的选择必须在安全体系结构内进行。安全体系结构是整个信息系统体系结构的一部分。安全体系结构描述了信息系统安全措施的合乎逻辑的安排与布局，它考虑了安全措施的技术方面，同时也涉及非技术因素。

所有的安全措施都需要由管理活动来激活其效能并维持其有效运行，很多安全措施的

维护(例如更新、功能增强)需要行政的强力支持。在选择安全措施的过程中这些因素必须予以考虑。

重要的是,安全措施的选取必须满足预期效能并且不导致不适当的管理开销。安全措施的选取不得造成用户活动和系统管理过程的重大变动。

2) 残留风险与可接受的风险

在实施选定的安全措施后,系统仍然存在残留风险。这是因为一个系统不必也不可能做到绝对安全或零风险,因此会有意或无意地留下一些未予保护(比如,假定风险很低,或相对于要保护的资产的价值来说,被推荐的安全措施成本太高,因此不必保护)的地方。

残留风险评估的第一步是复审所选安全措施实施后的实际的安全效能与设计的效能之间的差异;第二步是对设计时就有意或无意留下的某些安全脆弱性面临的风险进行估算,然后综合得出残留风险。在此基础上将残留风险分为两类,即可被组织接受的和不可接受的。

可接受的风险一般理解为对这种风险或是可以控制的,或风险的损失在预期内(风险发生的概率小或损失小,风险发生后可应对或对抗风险的成本不高);不可接受的风险则不能被容忍,应该考虑额外的安全措施以限制那些不可接受的风险带来的影响或后果。

总之,对残留风险是否可以接受还应进行评估。

5.4.2 安全管理和风险分析

信息安全管理从制定信息安全规划开始,规划的主要任务是确定信息系统总体安全目标、方针和策略,以此作为组织的信息系统安全管理的纲领性指导文件。

在信息系统安全目标、方针和策略的指导下,信息系统安全管理的活动包括识别信息系统资产、资产的脆弱性及其面临的威胁,威胁行为实施成功后的影响,按脆弱性分布和威胁路径确定风险的分布及强度,由风险分布和强度导出信息系统的安全需求,设计满足安全需求的信息系统安全保障体系,设计和实现信息安全解决方案,以及对信息安全措施的配置、运行和维护进行管理等。这些信息安全管理活动是一个有序的逻辑流程,即信息系统生命周期的安全管理过程。

在这一过程中,如遇与信息安全管理有关的法律法规发生变化、信息系统的业务或系统组件发生变化、信息系统的运行环境发生变化、安全保护措施发生变化等情况,均应对变动部分可能引起的新的风险进行评估,如存在不可接受的风险,则应对安全措施予以调整或增加新的安全措施(包括管理的和技术的),必要时应重复前段所述过程活动。

在信息安全的实际管理中,一般做法是在组织的信息安全目标、方针和策略指导下以风险分析和管控为主线开展管理活动,包括处理各种后续(跟踪)管理活动,例如维护、安全遵从性检查、变更管理、监控和安全事故处理等。图 5.9 列出了基于风险分析的信息安全管理所涉及的各部分活动内容。

5.4.2.1 信息安全的目标、方针和策略

一个组织对信息系统的安全进行规划时要制定组织关于信息系统的安全、方针和策略。这里的目标(指要实现什么)、方针(如何达到目标)和策略(为达到目标需遵循的规则和指令)应该在一个组织的每个层次和每个业务单位或部门中进行定义。为了获得高效能的信息安全保障,有必要针对组织的每个层次和业务部门的实际需求确立不同的目标、方针和策

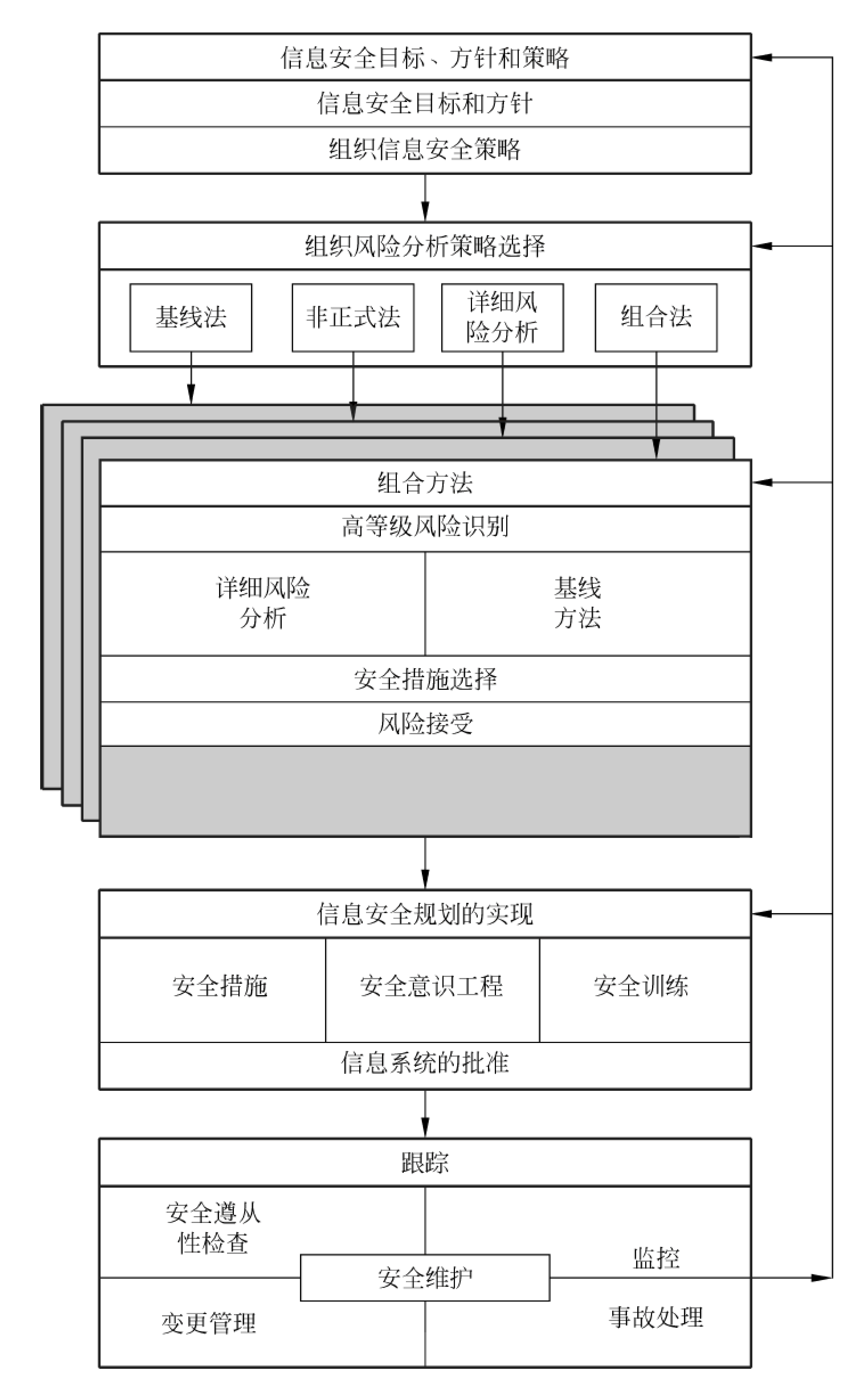


图 5.9　基于风险分析的信息安全管理过程

略。重要的是使多个层次和业务部门的这些目标之间保持定义和概念的一致性，因为许多关于脆弱性、威胁和安全措施的管理信息是需要并可能实现共享的。

组织的信息系统安全目标指的是信息系统及其资产的机密性、完整性、可用性、可控性等安全特性受保护的程度（即安全保护等级）要求；对数据（信息）、组件和系统的备份要求，信息系统发生安全事件后按危害程度分类实现快速恢复的要求；信息系统存在的残留风险的基线（即底线，一个人为设定的阈值）要求，即超过这一基线的风险是不可接受的。在信息安全规划文档中涉及描述这些安全目标时，一般应采用自然的社会化管理语言，避免使用过于技术性或学术型的语言，这样有利于组织内部各类与信息安全管理有关的人员之间的沟

通和交流。

信息系统安全方针指的是实现安全目标必须遵从的方式方法，包括实现信息系统及其资产机密性、完整性、可用性、可控性保障的技术标准和工程方法；数据(信息)、组件和系统备份的保存方式、保存的场所与保护的方法，以及当安全事件发生后按危害程度选择恢复对象(数据(信息)、组件和系统)和实现快速恢复的方法；将风险评估结果与基线比较，判断信息系统的残留风险与可接受基线的符合程度。

信息系统安全策略指的是实现信息系统安全目标采用的一系列规则和指令。这些规则和指令包括行政管理条例和技术操作规程，为信息系统内涉及安全的所有员工制定的行为规范。组织的信息安全策略必须与组织的安全策略、业务策略保持一致，这样才能在实施时获得所需的系统资源，并且能确保在各种不同的系统环境里保持一致的安全保护方法，必要时可为每个或某些信息子系统开发独立的和专门的安全策略。

1. 合理的安全目标和方针

作为信息安全管理过程的一步，应考虑的问题是"多大的风险水平对这个组织是可接受的?"。正确的可接受的风险水平和合适的安全保护等级是安全管理成功的关键。所需的安全保护等级是由组织的信息系统安全目标推断的。为了评估这些安全目标的合理性，首先应该考虑信息系统及其资产对这个组织的价值，包括评估一个组织的业务对信息系统的依赖程度，必须考虑的因素如下：

- 识别信息系统的运行环境和法律法规约束；
- 识别信息系统对组织开展的业务和自身管理的重要程度；
- 识别出那些必须在信息系统帮助下才能完成的业务和管理任务；
- 识别出那些必须依赖信息系统处理的信息的精确性、完整性或可用性才能实现的新业务或更强的业务能力(例如快速、准确的分类统计)；
- 识别出那些被拥有和使用的数据(信息)遭到泄露或破坏后的严重后果；
- 评估各种安全事件可能造成的后果，识别出其中后果最严重的安全事件导致的后果；等等。

理解这些问题可以帮助用户建立一个组织的安全目标。例如，如果一个组织的业务中的一些重要或很重要的部分必须依赖于精确的或最新的信息，那么这个组织的一个安全目标就是要确保信息在系统中处理时的完整性和实时可用性，进一步说，在评估安全目标的合理性时还要考虑实现重要的业务目标和保护它们的安全之间的关系。

信息系统安全方针用一般社会性和管理性语言来描述一个组织应如何实现它的信息安全目标。方针的描述应与安全目标的描述具有对应性，这些描述可能很具体(例如对某个信息体采用加密措施保护机密性)，也可能很宽泛(例如对某子系统或组件采用完整性保护措施以防篡改或假冒，或者将整个系统或某(些)子系统与外部进行隔离，等等)。

作为安全方针的一个示例，假设一个组织的业务必须保持持续不间断的服务能力，其安全目标是需要对与该业务有关的整个系统维持一个高等级的可用性水平，在这种情况下，安全方针所提出的办法可能就是直接通过在整个系统范围设计一个查、杀和防病毒体系(网络防病毒与主机防病毒相结合的)系统，以及快速恢复系统，以此维持系统业务的连续可用性。

为了说明安全方针的广泛意义，假设一个组织的业务是出售信息服务，那么这个系统必

须有一个更宽泛的信息安全目标，以向潜在的顾客证明其系统除了具有服务能力外，还具有让大家放心的安全性。这种情况下的安全方针除对系统本身进行必要的安全保护外，还必须邀请具有社会信誉度的可信任的第三方来证实其安全性。

具体的或宽泛的安全方针的其他选项可以包括：

- 对信息系统资源进行分类识别；
- 在整个组织范围内采用风险分析方法；
- 组织范围内的信息敏感度分类方案；
- 在连接到其他组织的信息系统前需要审核并满足安全连接的方法；
- 能被普遍应用的事故处理方案。

2. 适用的安全策略

一个组织的信息安全策略是实现安全目标的一系列规则和指令，应在组织的信息安全目标和方针基础上产生。建立和维护信息安全策略需要保持与组织的业务策略、安全策略、信息策略以及法律法规的一致性。在制定组织的信息系统安全策略时，还应充分考虑组织的文化、环境和机构的特点，因为它们会影响安全策略的选择，例如，一些安全操作规程可能很容易在一种环境下被接受，但在另一环境中完全不被接受。

在制定组织的信息安全策略时，以下职能部门的代表应该参加：

- 审计；
- 财务；
- 信息系统管理和维护；
- 公共事务基本设施（例如负责建筑、供电和空调的人员）的管理和维护；
- 人事；
- 安全；
- 业务高级管理层。

组织的信息安全策略的详细程度根据安全目标和一个组织为实现这些目标而采取的方针决定。

组织的信息安全策略至少要描述：

- 适用范围和目的；
- 覆盖组织和个人的责任和权限的管理规范；
- 用来确定安全措施实施优先顺序的规程；
- 组织要求的确定安全等级和接受残留风险的规程；
- 访问控制的一般准则（对建筑、房间、系统、信息的逻辑访问控制和物理访问控制）；
- 为提高遵守操作规范的自觉性，在组织内开展安全意识教育培训的规程；
- 检查和维护安全的规程；
- 对一般员工的安全管理制度；
- 把策略中的规则和指令传达到所有有关人员的流程；
- 对策略进行复核的规程；
- 对策略的更改进行控制的规则。

在对组织的信息安全策略进行描述时，必须考虑以下因素：

- 组织的信息系统的安全目标和方针；

- 组织范围内的信息安全管理模型和管理流程；
- 必须遵从的技术标准；
- 安全措施的实现步骤；
- 后续(跟踪)活动。
  - 安全遵从性检查；
  - 安全措施的监控；
  - 对信息系统的运行进行监控；
  - 安全事故的处理。
- 雇用组织外安全顾问的预设条件；
- 外包工程和委外合同的管理规程。

为了保证与安全管理有关的方方面面在实施中得到足够的支持，组织的信息安全策略应获得高层管理部门批准。

组织的信息安全策略应规定为所有管理人员和员工编写并分发有关操作规程。这可能需要每个员工在接收文件上签名，承诺其在组织内的安全责任，使安全策略既反映组织的管理需求，又考虑策略执行者在权力和责任之间的平衡。进一步，应开发和实施一个与此相应的安全意识和培训活动的计划。

组织应指派专人(通常是信息安全官员)负责组织的信息安全策略的制定和监督实施，同时负责有关的后续活动的协调，包括安全遵从性检查的评审、事故和安全脆弱性的处理，以及根据这些活动的结果可能需要对组织的信息安全策略进行变更或调整等事项。

5.4.2.2 风险分析方法

信息系统风险分析方法一般有 4 种，分别是基线法、非正式(规)法、详细风险分析法和组合法。

1. 基线法

这是一种在信息系统中基于基线保护的应对风险的方法，实际上并不逐一地进行具体的风险分析。假设一个组织的信息系统只有在实施某种等级的安全保护措施情况下才能获得最佳的安全费用效率比，那么这种信息系统宜选择基线法来反映信息系统需要的大多数保护，然后针对其中采用基线保护措施未能控制的风险额外地配置相应的安全措施予以应对。

具体做法是，先建立一个基线安全措施目录，包括若干组不同安全等级的最少数量的安全措施集，分别对应一个组织的所有或一些信息系统的安全保护，选取安全措施目录中某一组安全措施为信息系统建立合适的基线保护。目录中的每一组安全措施均可以满足某一安全等级的保护需求，对抗信息系统中最常见和最普遍的威胁。通过比较分析，可以调整基线保护的等级来适应组织的安全需要，这里不需要对脆弱性、威胁和风险进行对应性的完整评估。

基线法的使用减少了组织在执行风险评估时所需的安全投入。

基线安全措施目录要详细说明需要用到的安全措施的效能和适用方法，或者给出安全措施适用保护对象的说明或建议。基线安全措施目录可由具有技术能力的组织自己定制，也可以由第三方的信息安全咨询服务公司在国家有关技术规范与标准指导下编制，供各类信息系统选择。

基线法的优点如下：

- 风险分析和风险管理所需要的资源数量最小，选择保护措施时耗费的时间和工作量最少；
- 基线保护措施是一种效费比高的解决方法。如果组织的大量信息（子）系统都在普通环境下运行，很多（子）系统都可以简便地采用基线方法。

基线法的缺点如下：

- 如果基线水平设置得太高，那么整个信息系统的安全保护成本可能会抬高；
- 如果基线水平设置得太低，那么信息系统中某些部分的安全保护等级可能无法达到，从而导致不可接受的风险；
- 在对与安全相关的变更进行管理时可能出现困难。例如，如果一个系统升级了，就很难评估初始的基线保护措施是否足够。

2. 非正式（规）法

这种方法是对信息系统中的所有部分（组件、子系统）采用一种非正式的，但却实用的风险分析。它不是基于结构化的方法，而是利用个人的经验和知识识别出主要的风险及其分布情况。当组织内部没有可以胜任这一工作的信息安全专家时，组织外的信息安全专家们也可以受委托进行类似分析。

这种方法的优点是进行这种非正式的系统风险分析不需要学习更多的技能，而且比详细的风险分析快捷和简单，所以这种方法适用于小型企事业单位的信息系统，比较经济实惠。

这种方法的缺点如下：

- 由于分析没有采用结构化的方法，所以可能漏掉一些风险或风险区域；
- 保护措施只是针对已被识别的脆弱性、威胁及影响所评估的风险，从而进行配置的，而没有考虑到由于个人经验的局限性导致未被识别的脆弱性和潜在威胁；
- 由于采用非正式的方法，分析结果可能受风险评估人员的主观因素和个人偏好的局限；
- 很难证明根据这种风险评估方法所采用的保护措施是否合理和充分，因此会给残留风险的评估带来不确定因素；
- 由于在安全措施的选择上缺乏调整余地，所以安全措施的费用也很难调整；
- 在不进行风险的重新评估的情况下，如果系统的变更与安全相关，很难对这些变更引起的风险进行管理。

基于以上缺点，这种非正式的风险分析方法对安全保护要求较为严格的大中型信息系统并不是一个有效的方法。

3. 详细风险分析法

这种方法包括对信息系统资产的识别、对资产脆弱性和面临的威胁及影响的系统性分析过程。这种风险分析方法是一种结构化的分析方法，通过识别资产的风险给出信息系统的风险分布及其强度（一个以序列等级表示的序列值）的详细列表，为导出信息安全需求、识别和选择安全保护措施提供准确的适用对象，从而可以保证信息系统所属组织通过风险管理可将风险降低到可接受的程度。

详细风险分析过程如图 5.10 所示。

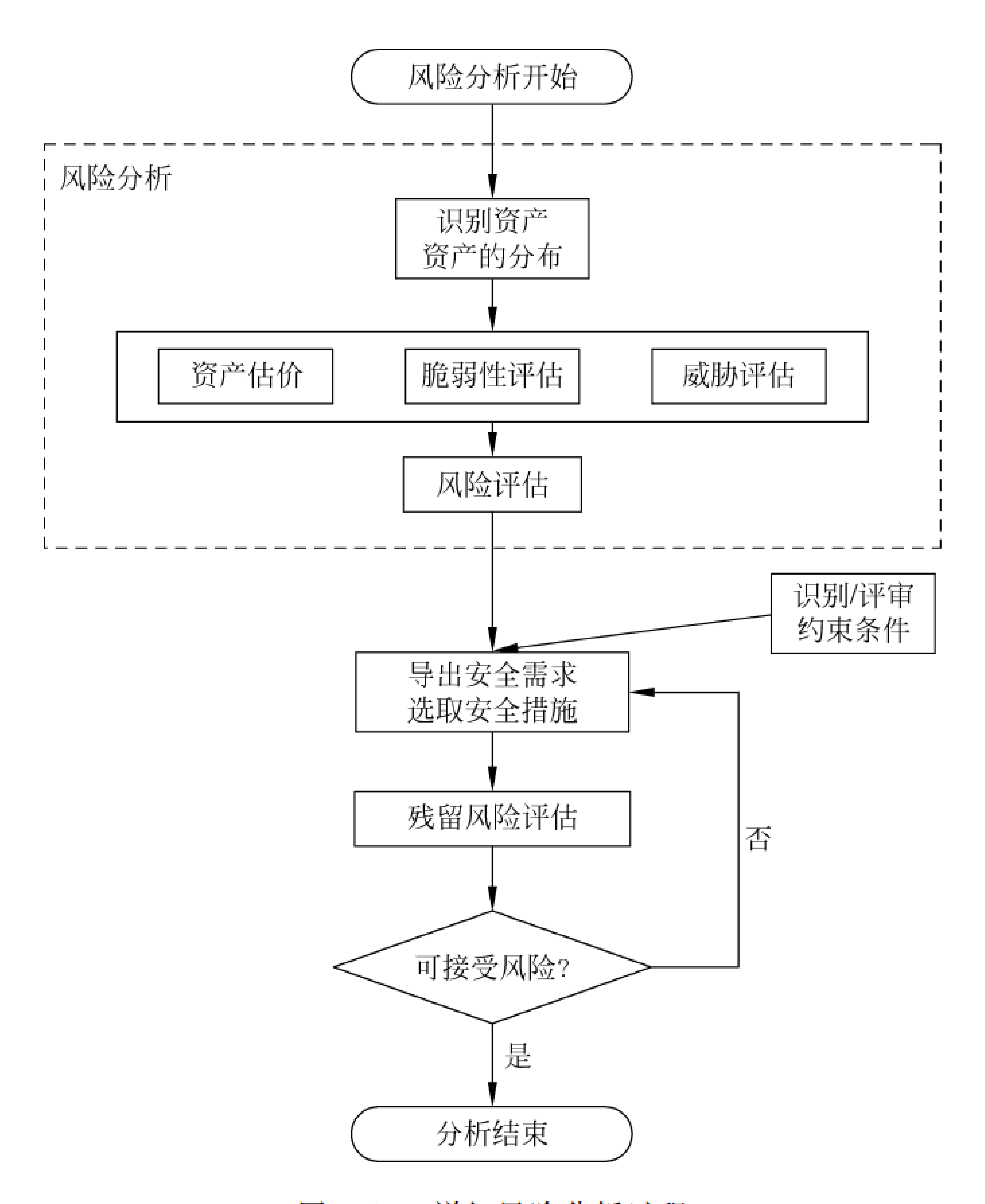


图 5.10　详细风险分析过程

详细风险分析的步骤描述如下。

1）资产识别

资产是信息系统中对组织有价值的信息系统构成要素(即资源)。在一般情况下,对信息系统资源和资产并不做严格区分。一个组织为信息系统资源确定价值,并且对它进行保护。对资产进行识别时,首先要识别信息系统资源(即信息系统构成要素),这里所说的信息系统资源不仅是由数据(信息)、硬件和软件组成的网络信息系统中的要素,而且包括设计、建设、管理和使用这些信息系统的人以及运行环境。资产类型包括:

- 数据/信息体(例如包含各种类型的数据、产品的信息等);
- 硬件(例如各类计算机及其外围设备,各种读/写存储设备、网络交换与通信设备、传输媒体和通信终端设备等);
- 软件,包括管理、控制、通信、存储和业务应用程序(例如主机和网络操作系统,管理协议、通信协议、数据库管理系统,文字处理程序,为特定业务开发的应用程序等);
- 固件(例如软盘、只读存储器光碟、可编程只读存储器和移动存储器等);
- 文档(例如组织的各类业务文档和归档档案,合作合同、管理的和技术的资料等);
- 软件产品;
- 服务流程(例如信息服务和计算资源共享);
- 服务过程中的秘密信息(例如支付服务流程和方法等);

- 运行环境；
- 信息系统设计、建设、管理、使用和维护人员；等等。

在实际工作中，风险分析人员应针对信息系统的实际情况，按照上述列项（而不是照搬上列款项）识别出需要保护的信息系统资产。

需要保护的所有资产都必须进行识别和标识，应保证需要识别的资产不被遗漏。

2）资产价值的估计

列出信息系统的所有资产后，应该给这些资产确定价值，这些价值代表了资产对一个组织业务的重要性。基于组织的业务需要，对资产的识别和估价是风险分析中的重要环节。确定了价值的信息系统资产即是风险分析中需要关注的资产。

对信息资产价值的估计应该从组织内那些参与业务计划、财务、信息系统建设和其他相关活动的人中寻求支持，以使每一个资产估值是合理的。资产价值应与获得和维护这些资源的费用有关，还应与这些信息系统资产的机密性、完整性、可用性、可确认性和可靠性的丧失而造成的潜在的业务负面影响有关。然而并不存在一种直接的或简单的方法对所有的资源确定经济上的货币化价值，因此还应同时采用非货币化的计算方法，将对组织业务产品或服务质量、社会效益、组织信誉等的影响因素考虑到对资源的价值评估中，否则将不能准确估计所需安全保护等级以及组织为保护这些资源应投入的安全成本。

估价尺度可以是低、中和高 3 个等级数值，或者 5 个等级数值，即可忽略的、低、中、高、很高，还可以有其他的确定资产价值的更细粒度的度量尺度。不管采用什么度量方法，以下情况所导致的影响必须在估价中予以考虑：

- 违反法律或法规，或错误理解、使用法律法规引起的负面影响；
- 业务性能下降造成的损失；
- 信誉或名誉损失所产生的负面影响；
- 与个人信息相关的机密性和完整性损坏；
- 员工安全受到的危害；
- 商业信息的机密性和完整性受到破坏；
- 资金或虚拟资金损失；
- 业务活动的中断；
- 环境安全受到破坏；
- 信息系统中其他在估价时应考虑的情况，例如在实现业务或其安全保护措施时，采用了不适当的技术措施（典型例子是在加密技术中引入了未经国家允许的算法）可能带来的后果。

在这一阶段需要强调的是，估价的方法不仅允许进行定量的计算，而且在进行定量计算不可能或不合逻辑时，必须进行定性的评估（例如生命丧失的潜在损失、公司信誉损失），并对所用的估价尺度给出解释。

对某一（些）资产的价值进行估计可能还要与信息系统所属组织的规模和特点建立联系，例如一定数量的资金损失对一个小公司来讲可能是致命的，但对一个大型公司来讲也许并不重要，甚至可以忽略不计。

某一（些）资源对其他资源的依赖性也需要识别，因为这种依赖性可能影响对资产价值的评估。例如，在整个信息处理过程中必须保持数据的机密性，这样数据处理过程后的机密

性就依赖于被处理数据最初状态时的机密性，如该数据在处理前的存储设备缺乏保护，那么不管该数据在处理过程中采用什么保护措施都是无济于事的；又如，一个业务过程（例如ATM机存/取款过程）依赖于某个程序（例如数据库管理程序）产生的该用户数据的完整性，那么该程序输出的数据就必须是完整和可靠的；再如，信息的完整性依赖于存储和处理该信息的硬件和软件系统的安全性。进一步说，硬件的可靠运行也依赖于电力供应，可能还有空调等环境条件。因此，有关依赖关系的分析将对特定脆弱性和相关威胁的识别提供帮助，这将有助于将资产的真实价值（通过依赖关系）分配给有关联关系的那些资源，并确保这些资产得到合适的保护。

依赖于其他资产（彼资产）的资产（此资产）所具有的价值可用以下方式修正：

- 如果那些依赖于彼资产（如数据）的价值低于或等于此资产（如软件）的价值，则此资产的价值保持不变；
- 如果那些依赖于彼资产（如数据）的价值较高，则要根据下面的考虑增加此资产（如软件）的价值：
  - 依赖的程度；
  - 与之关联的其他资产的价值。

一个组织的某些资产可能被某个资产重复使用或被多个资产共同使用，例如软件程序副本或者大量的不同应用数据存储在同一设备中，在进行资产评估时必须进行关联性考虑。

信息系统资产识别过程的最后输出是一个资产及其价值的列表，其中价值与泄漏（机密性保护）、修改（完整性保护）、不可用和破坏（可用性保护）造成的影响以及为降低或消除这些影响而采用安全保护措施的成本等相关。

3）脆弱性评估

脆弱性评估的对象是物理环境、组织、规程、人事、管理、行政、硬件、软件或通信设施等信息系统资源或资产的弱点或缺陷。这些资源的弱点或缺陷可能会被威胁主体开发利用，进而导致对信息系统资产和业务的危害。脆弱性的存在本身并不造成危害或损害，但当存在能利用它的威胁时，脆弱性的问题就必须考虑。没有相关威胁存在的脆弱性不需要实施安全保护措施，但是需要监视和识别可能出现的变化。应该注意，一个未被正确实施或虽实施了但效能不充分的安全措施，或没有正确选用的安全措施，本身就是一种脆弱性。

脆弱性一般与资产的特性或属性有关，也可能因不能满足在购买或制造时所承诺的功能/性能指标在使用后出现脆弱性或缺陷。例如，一个EEPROM（电可擦除可编程只读存储器）的特性之一就是上面能存储信息并可以被擦除和替换。这本是一个EEPROM的设计准则，然而，这个特性也意味着可能对存储在EEPROM上的信息进行未授权的修改或破坏。

识别和评估可以被威胁利用的脆弱性，并评估其弱点或缺陷的等级，也就是被威胁开发利用的容易程度和可能造成的损失程度。脆弱性评估者应包括资产的所有者和使用者、设备专家以及硬件和软件方面的专家。脆弱性的典型例子如下：

- 未受保护的连接（例如接入因特网）；
- 未受训练的用户；
- 不按规定选择、使用和保管口令，以及口令字长度过短或易于猜测，或将口令字暴露在桌面上等；

- 在公共区域使用未加屏蔽的信号线传输数据；
- 没有信息或软件的备份；
- 建筑物或机房位于易遭受洪水、泥石流等侵害的场所；等等。

重要的是在评估资产的脆弱性时还应标识其严重程度，即它们被威胁开发利用的容易程度和可能造成损失的程度，可用低、中、高来表示，或用其他表示等级的方法来度量。例如，一个系统可能存在对其资源进行冒用或滥用的脆弱性，那么缺少用户身份鉴别机制，冒用用户身份的脆弱性就会很高，但对滥用资源（即不合理地使用资源）的脆弱性却会低，因为即使不需用户鉴别，用户还需对资源有访问权才能成功访问，因此资源被滥用的可能性也是有限的。

脆弱性评估的输出结果应该是一个列表，包含脆弱性、对应的威胁及脆弱性被利用的容易程度和造成的损失程度等内容。

4）威胁评估

威胁是利用信息系统资源的脆弱性危害信息系统及其资产的潜在的因素。威胁在条件具备时就会以一定方式影响或危害信息系统，导致意外事件发生和产生负面影响。威胁可能是自然的或人为的因素，威胁的出现可以是偶然的或蓄意的。无论是偶然的还是蓄意的威胁的来源都应该予以识别，并对实施威胁获得成功的可能性予以评估。

威胁评估的输入应该从以下方面获得：资产的所有者和使用者、人事部门员工、设施规划和信息技术专家，以及组织的安全管理人员等。其他组织，如国家有关安全管理政府机构和社会第三方安全咨询服务机构也可以为威胁评估提供帮助，例如提供威胁的统计资料和共享威胁数据库（例如潜在威胁目录），参考其他组织或国际机构的威胁目录也是有益的。

一些普遍的威胁的表现形式如下：

- 误操作和滥用信息资源；
- 信息欺诈和偷窃；
- 员工蓄意破坏或泄露数据；
- 未经允许的黑客技术行为（例如伪装身份、入侵和信息阻塞等）；
- 与情报有关的信息收集活动；
- 信息监听和侦听活动；等等。

在使用威胁目录或此前的威胁分析结果时，应该意识到威胁的方法和路径是在不断变化的，特别是当业务环境或信息系统发生变化时。

在确认了威胁源（威胁行为的主体）和威胁目标（可能会受到该威胁的资产）后，评估威胁时应该考虑下列因素：

- 威胁出现的频度（根据经验、统计资料等进行粗判）、持续的时间等；
- 威胁的动机，被觉察或估计到的威胁者所具有的潜在攻击能力，可能利用的用于攻击的资源，以及信息系统资产对威胁源的吸引力和自身的脆弱性程度；
- 威胁源可利用的地理性因素（如从逻辑或物理角度靠近被攻击的对象），极端天气出现的可能性，以及能引起人类错误和设备故障的各种因素。

根据对威胁评估准确性的要求，可能需要将受攻击的资产定位到系统的具体部件上，并且将威胁与部件对应地关联起来。例如，可能受攻击的物理资产是“数据服务器”，当这些服务器被确认处于不同的地理位置时，则攻击对象应具体地定位为“数据服务器 1”、“数据服

务器 2”……。类似地，可能受到攻击的软件资产是一个“应用软件”整体，但这一软件却被分成若干子系统（或模块）分布于信息系统中不同的硬件上时，则攻击对象应定位于相应的子系统所安装和运行的硬件上。又如关于数据资产的例子，一个记录嫌疑犯证据的“犯罪记录”的文档是一个整体，但是却被分成“犯罪记录文本”和“犯罪记录图像”分别存储在不同的服务器上。很显然，在评估威胁时应将可能受攻击的对象定位于不同的服务器上。

威胁评估完成时将会有一个列表，包含已识别的威胁，可能受它们攻击的资产或资产组及其脆弱性的对应关系，以及以某种评估尺度（比如高、中或低）表示的威胁严重性的度量。

5）风险评估

在对信息系统资源分布进行识别，对资源的价值进行估算，识别信息系统资产的脆弱性分布及程度，进而评估针对信息系统资产脆弱性的威胁实施的可能性及损失程度后，风险分析的任务就是识别和评估信息系统及其资产的风险分布及强度。

对于风险的确定，需要根据处于威胁中资源的价值及资产的脆弱性、资产的脆弱性被威胁利用的难易程度，以及威胁针对脆弱性实施攻击的成功可能性和损失（包括有形的和无形的、货币的和非货币的）进行综合判断。

风险可以用等级来度量。影响风险等级的因素有资源的价值、脆弱性的程度、威胁的强度及利用脆弱性攻击成功的难易程度、攻击成功后给信息系统造成的各种形式的损失总和。在具体分析中，应对风险影响最大的那些因素予以特别关注。

风险评估的结果应该是一个已度量风险的列表，包括风险分布在系统中的资产点及风险等级、风险的表现形式（信息泄露、修改、不可用等）、风险造成的损失形式（有形的、无形的，货币的、非货币的）等内容。

6）安全需求分析和安全措施的选取

按照风险评估列表中风险对应的保护对象（即资产），通过在信息系统的网络层、传输层、应用层、系统层和用户层上的某一层或某几层上选择安全保护机制（技术），然后转换成安全保护措施，并将安全保护措施转化成（包括以管理和技术形式出现的软/硬件）安全设备或系统，分别部署在信息系统的合适位置，覆盖整个风险分布区域，这就是安全需求分析必须解决的问题。

在采用安全措施实现安全机制时，其形式可以是一个功能模块、一个子系统、一个功能组件，这些可以嵌入到某一应用进程中，也可以组装到一个软/硬件系统中。有的安全措施可以为多个保护点提供对抗风险的能力，有的资产（由于存在多种风险）则需要多种安全措施的保护。特别需要强调的是，不可期望某一个安全措施可以对抗信息系统的所有风险。

安全措施对抗风险的策略是通过阻止、降低、规避或转移（嫁）对信息系统资产实施的入侵、攻击和破坏资产的行为，将风险降到信息系统所有者和管理者可以接受或控制的水平。

在安全措施的选取过程中，还需遵从必要的约束条件，特别是那些涉及国家安全和主权的规定，例如典型的法律约束是不可选取未经国家允许的国外的或自主开发的密码设备或算法。

关于安全措施选择方法的详细介绍，见第 5.4.3 节“安全措施的选择与实施”。

7）可接受风险

所选择的安全措施的实施无疑可以降低已有风险，但信息系统总会有残留风险。这些

遗留在信息系统中的风险有的可能是所有安全措施都未能或不必应对的,例如在一般商用信息系统中,对密码算法破译这类风险就不必追求不计成本的高强度的密码算法,又如在应对涉密信息通过互联网泄露的问题上就没有必要为此将整个系统与互联网断开;有的则可能是在风险分析时漏掉的。

问题不在于这类残留风险是否一定是存在的,而在于残留风险到底还有多大或是否可控。在选择并实施安全措施后,应对信息系统的残留风险进行评估。评估的结果将与在信息系统安全规划时所确定的可接受风险进行比较,比较的结果会有一个差值(即安全风险容差)。只有当风险容差在预期范围内,残留风险才是可以接受的或可控的;否则残留风险是不可接受的,必须有针对性地调整安全措施或增加安全措施,并再次进行残留风险的评估(包括必要时进行测试),直到符合要求为止。需要指出的是,风险评估的含义包括对风险的理论评审和在必要时进行技术性测试。

综上所述,详细风险分析方法的整体优势是基线法和非正式(规)法不可及的,但并不要求也无必要对所有信息系统的风险分析都使用这种方法,因为风险分析方法的选择原则应服从适度安全原则(详细风险分析方法投入很大),不计成本或脱离信息化发展现实去过度追求安全保护不仅无益,而且有害。

这种方法的优点如下:

- 对信息系统资产而言,都有量身定制的安全等级保护措施满足其安全需求;
- 对与信息安全相关的系统变动的管理可以从详细风险分析结果中获得知识。

这种方法的缺点是,要得到较好的详细风险分析结果,需要付出相当多的时间、精力和费用,并且要求分析人员具有相当专业的知识。因此,对信息系统不加区别地使用详细风险分析方法是不明智的。

4. 组合法

这种方法是将基线法和详细风险分析法有条件地结合起来,从而实现真正意义上的最佳安全效能与成本比的风险分析方法。具体做法是首先将那些对业务运营来说有较高风险强度或需要重点保护的子系统(或组件)识别出来。基于这些识别出来的结果将信息系统分为两个子类,一类需要使用详细风险分析法才能使其达到合适的保护,另一类则是只用基线法保护就足够了。这就是信息系统内的分类或分域保护的基本思想,可以避免对面临不同威胁的信息系统资产采取同一安全保护强度措施的做法,为解决信息系统内一部分资产受到过分保护,而另一部分资产却保护不够的问题提供了一种可选方法。

显然,组合法综合了基线法和详细风险分析法的优点,它在安全保护效能和成本开销之间维持一个最佳平衡,既节约安全资源,又满足了既定的适度保护要求。

这种方法的优点是将安全资源(行政的、技术的)和资金用在最需要的地方,并可获得安全保护的最佳效能费用比。

这种方法的缺点如下:

- 如果对信息系统中的高危风险点的分析判断不准确,或需要详细风险分析法才能确定的风险点被遗漏,或某个(些)子系统或组件的风险被严重低估,则可能导致无法预测的后果;
- 对从事风险分析的专业技术人员必须具备的信息安全知识和职业素质有更高的要求。

对于大中型信息系统和重要信息系统来说，这应是最有效的风险分析方法。从近年来的风险分析实践来看，越来越多的组织较为成功地运用组合风险分析方法实现了对信息系统的适度安全保护，取得了明显的社会经济效益。

5.4.3 安全措施的选择与实施

对信息系统进行必要保护的安全措施是按照组织对信息安全的规划中确定的安全目标、方针和策略对信息系统进行风险分析后，根据风险分布及其强度予以选择和实施的。

以组合风险分析方法选择安全措施为例，为了选择适当的安全措施，有必要进行一些基本评估。评估对象包括：

- 信息系统的类型（单机，还是网络，网络的互连互通情况）；
- 信息系统的物理位置和周围环境条件；
- 已经部署的和计划中的安全措施；
- 评估所提供的信息对于选择“基线”安全措施是否足够，如不足够，是否需要增加评估选项进一步获得足够的信息，否则应选择详细风险分析方法来选择安全措施。

风险分析与安全措施的选择之间的关系如图 5.11 所示。

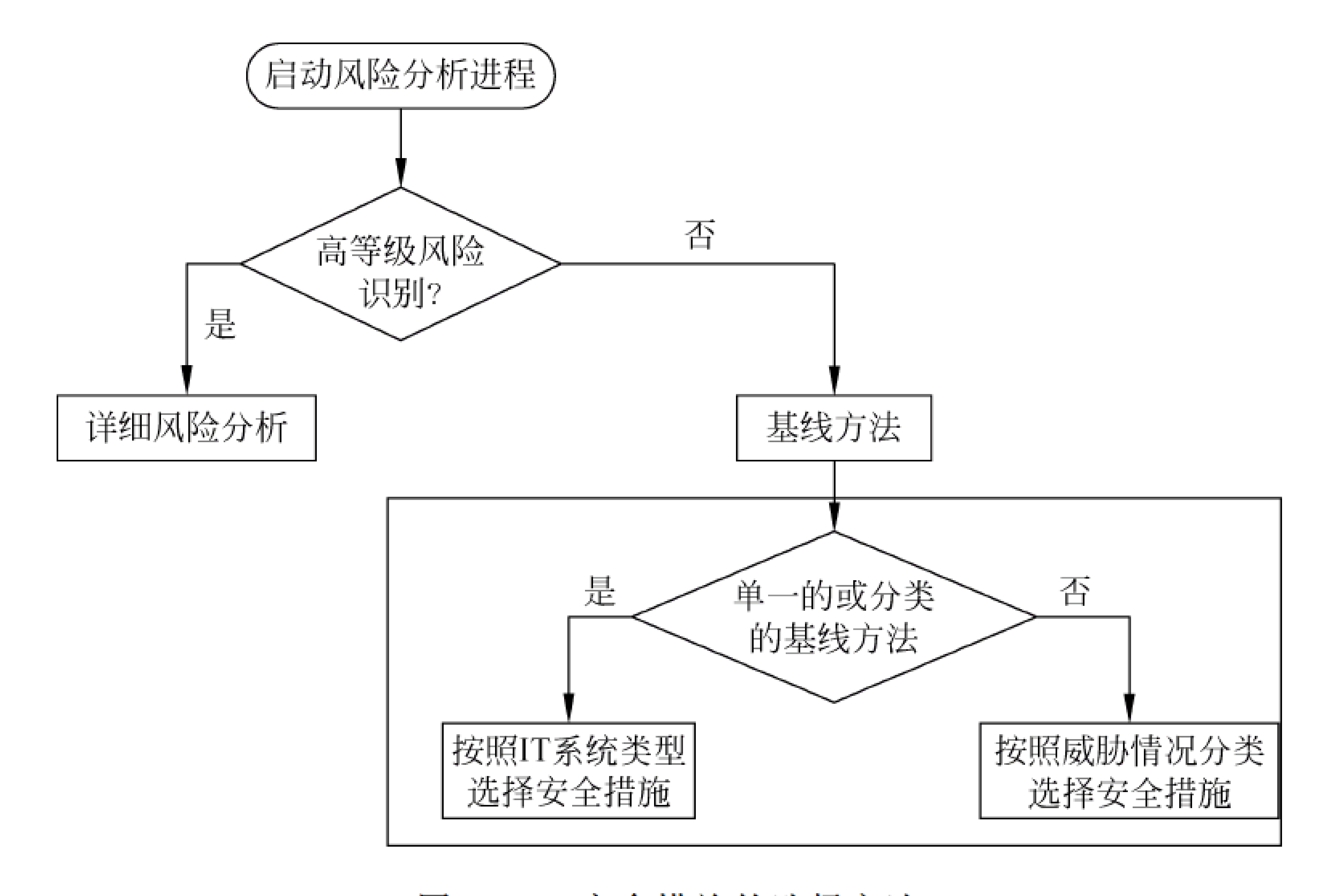


图 5.11　安全措施的选择方法

实施详细风险分析法可以对风险状况有一个全面、深入的结构化认识。如果组织的业务运行在很大程度上依赖信息系统或服务，或信息系统所处理的信息非常敏感，信息系统结构复杂，整体风险比较高，且其中的高危风险分布点相互覆盖和交叉情况严重，则应在详细风险分析的基础上选择安全措施，这样可以避免对一部分资产保护过度，而对另一部分资产欠保护的情况。

另一方面，对于一些高危风险相对集中且易于识别，或信息系统结构相对简洁且面临的整体风险较低的情况，采用基线法选择安全措施是较为简单易行的方法。这种方法即是为信息系统选择一套满足信息系统安全需求的最低保护标准的安全措施，也称为基线安全模式。在采用基线安全模式评估风险后选择安全措施时，必须考虑可以利用的安全资源、安全

保护重点以及所涉及的信息系统的业务保护类型和特点。使用基线法选择有下面两条途径：

- 根据信息系统的业务保护类型和特点选择统一的基线安全措施；
- 按照安全保护重点和威胁情况分类选择基线安全措施。

图 5.12 给出了根据信息系统业务保护类型或根据安全保护重点和威胁分类选择安全措施的过程，可以看作是对图 5.11 的补充。

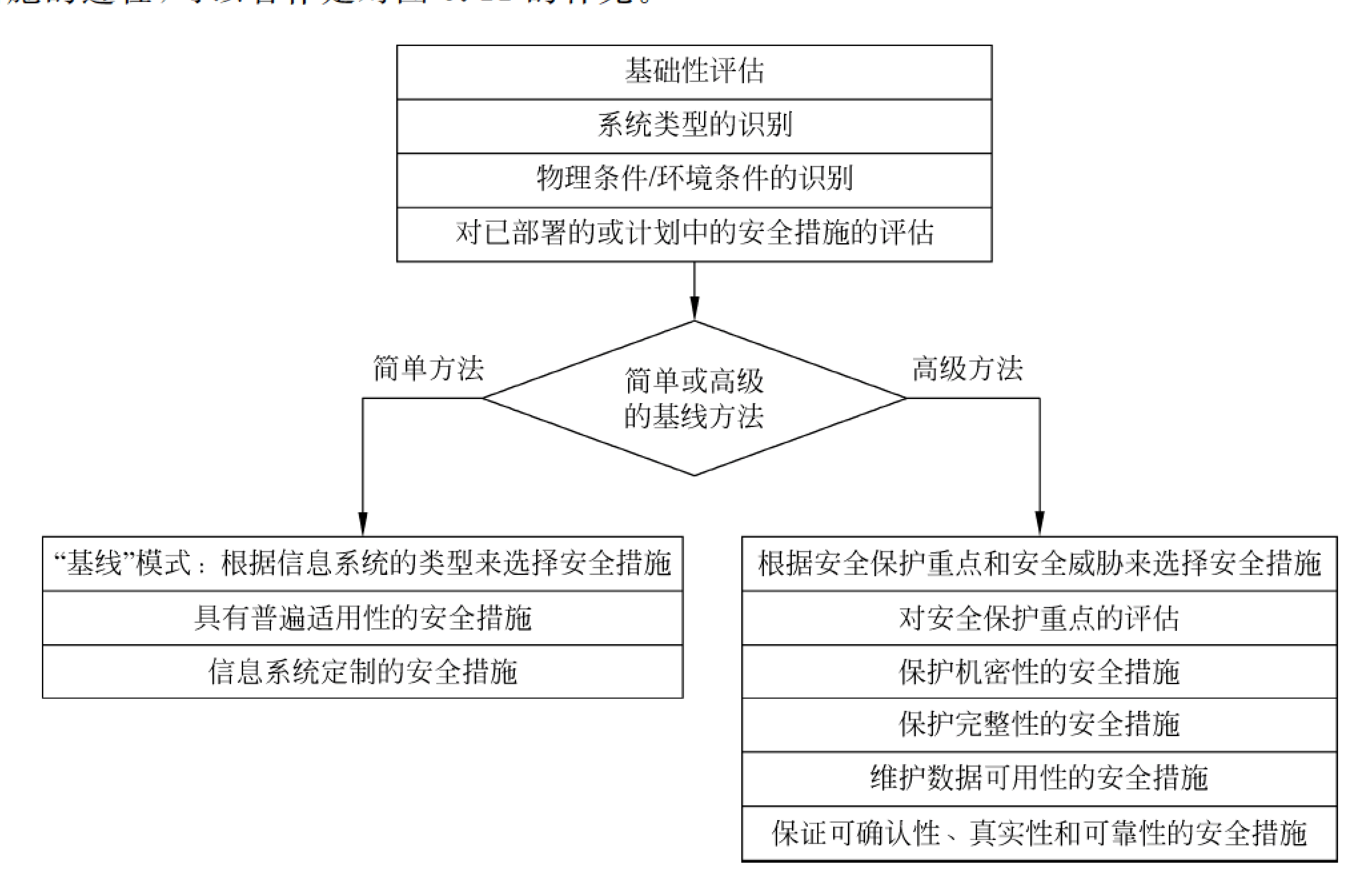


图 5.12　根据信息系统类型或安全保护重点和威胁选择安全措施

如果组织的业务运作以中等程度依赖信息系统或服务，或信息系统所处理的信息比较敏感，那么就需要更多的(分类)基线安全措施，在这种情况下，为了使所选择的安全措施有效地保护信息系统，最好是对所关注信息保护点的风险进行分类分析。

图 5.12 中的"高级方法"只是说明了应该对不同类型的风险选用不同的安全措施，这些安全措施可以是基线安全模式中分类的基线安全措施，也可以是根据详细风险分析后选择的各类安全保护措施。一般来说，详细的风险分析方法对于"基线"安全措施的选择肯定是有帮助的。

因此，组织在选择安全措施之前必须做的一个决定是只单纯地使用"基线"方法，还是把"基线"方法作为更广范围内的风险分析战略的一部分。在做此决定时需要知道的是前者的安全效果很可能要低于后者。如果考虑到安全措施选择过程中的成本、资源的耗费，以及对信息系统的适度安全保护水平，那么在一些安全要求不高的小型网络中使用"基线"模式是最具安全效能和成本比的。

如果一个组织决定要在其整个信息系统中或部分子系统中应用"基线"安全模式，那么需要决定组织的哪些子系统可以使用相同的"基线"，以及这种"基线"应该达到什么样的安全保护等级水平。在绝大多数情况下，使用"基线"安全模式仅能保证最低的安全保护等级，当涉及中等级以上的风险时还要实施额外的安全保护措施。而在有的情况下，"基线"安全

措施只是达到信息系统安全保护整体要求的必要条件，要使信息系统整体安全保护水平充分满足信息安全规划时确定的安全目标，可能需要根据风险分析的结果在“基线”安全保护措施实施后进行必要的调整或额外地增加安全措施。

在基线安全模式下，对组织或部门的“基线”安全措施目录进行编制、完善和归档通常是非常必要的。

5.4.3.1 基础性评估

在选择安全措施的过程中，需要一些信息系统的类型和特征的信息（例如单机 PC，还是连接到内部或外部网络的 PC，是独立的局域网还是与外部网络互连的网络），对建筑物、房间和物理环境等基础设施的信息，以及已有的安全措施效能的评估信息。这些信息对安全措施的选择和完善有着重大的影响。

1. 识别信息系统类型和特点

识别信息系统类型和特点的内容如下：

- 系统内独立的 PC 机、工作站或服务器；
- 通过网络相互连接但不共享资源的 PC 机、工作站或服务器；
- 通过网络相互连接并共享资源的 PC 机、工作站或服务器；
- 组织的网络与外部网络物理隔离；
- 组织的网络与外部网络逻辑隔离；
- 组织的网络与互联网连接，或与组织外的信息设备共享信息。

2. 评估物理环境

对环境的评估包括识别组织信息系统的位置和对周边环境的控制程度，识别组织机构环境中需要特别关注的安全风险，已有的或计划中的支持或保障物理环境安全的安全措施，并评估安全措施与物理环境安全要求的适应程度，这些工作对安全措施的选择是否成功至关重要。评估可通过回答下列问题进行。

1）建筑物和周边环境

- 建筑物的位置是有围墙的单独场所，还是毗连车水马龙的大街？
- 建筑物是独占还是共同占有？
- 如果是共同占有，那么与其他占有者的关系是否可控？
- 敏感/关键区域的周边情况是否可控？

2）对访问的控制

- 除组织的员工外，还有哪些人可以进入建筑物？
- 组织的信息系统资源所在区域与同一建筑物内其他区域是否有物理控制措施和访问控制制度？
- 在建筑物内适当的位置安装了视频监控系统吗？
- 建筑物结构的牢固程度如何？
- 门、窗户等设施的牢固程度如何？对它们采取了何种保护措施？
- 建筑物有保安吗？如果有，是每天 24 小时全天候保卫，还是仅仅在工作时间保卫？
- 建筑物或放有关键装备的房间是否配备了报警器？

3）已有的安全措施

- 对放置信息系统的房间采取了哪些保护措施？

- 在信息系统关键或重要资源放置场所配备了烟雾检测、警报和灭火设施吗？
- 在信息系统关键或重要资源放置场所配备了水/液体的泄漏检测装置、泄漏警报装置和排泄设施吗？
- 信息系统有不间断电源（UPS）和空调（对温度和湿度进行控制）等支持系统吗？

通过回答这些问题能够容易地识别出在物理环境区域里已存在的各种安全措施。例如当考察建筑物的门禁时，可以同时确认门锁以及其他物理访问控制措施。

3. 对已有或计划中安全措施的评估

在搞清信息系统的组件类型、特点及其物理环境情况后，应对其中已配置到位或计划中的安全措施进行确认，以避免重复选择安全措施，消除安全措施配置冗余可能引起的冲突；也有助于将已实现的或计划中的安全措施与所选择的安全措施的安全效能进行互补性和增强性的有机结合。

在选择安全措施时，必须考虑已有安全措施（包括已实施的和计划实施的）与新选择的安全措施之间的兼容性，避免新的安全措施与已有的安全措施之间发生冲突，或者不能顺利地运行和提供对系统的预期保护。

为了对已有或计划中的安全措施进行确认，下列活动是有帮助的：

- 查阅有关安全措施信息（例如信息系统安全设计方案和工程设计）的文件，如果安全管理过程的文档齐全，那么相应的文件中应该列有所有已有或者计划的安全措施的选取或实施的信息；
- 从信息系统有关人员（如信息系统安全官员、设计、施工或运维人员）和使用人员那里核对信息系统中那些已经运行和正在实施的安全措施的详细情况；
- 仔细观察信息系统内各项软/硬件形式的安全措施，将已经实现的安全措施与应该实现的新的安全措施进行比较，以便确定在实现的新的安全措施后是否存在遗漏和安全保护能力不足的情况。
- 复核已实现的安全措施是否正确地运行，以及与设计的安全效能的符合情况。

如果发现已有安全措施超出了当前的安全需求，可考虑或拆除某些组件或设备，或通过管理配置卸掉多余配置的安全措施。在决定拆除某些安全设备或通过管理配置卸掉某些安全功能时，必须认真评估这些行为对整体安全保护效果的影响，保证这些行为能提升信息系统运行效率和降低安全开销的同时，仍能确保信息系统的安全等级保护水平符合组织在安全规划中提出的安全目标。需要特别提醒的是，由于安全措施之间是相互影响的，去掉多余的安全措施可能降低整体的安全性，因此在做此决定时要十分谨慎和小心。

5.4.3.2 安全措施

这一节将对用来实施安全保护的安全机制和安全措施做一般性的介绍。在这些安全措施中，一部分是保护机制，另一部分是安全服务。在对安全措施进行阐述时，这里并不考虑选择方式。有一些安全措施可以使用任何方式进行选择，而有的则应该或只能通过详细风险分析方式来选择。

为了便于描述各种类型的安全机制和安全服务措施，这里引入了安全措施类别的概念。安全措施可大致分为管理性安全措施和技术性安全措施。其中，管理性措施指那些与组织所属机构属性有关的组织管理策略原则、组织的行政措施和法律约束活动等；技术性安全措施主要指以技术形式表现的包括以软件形式和硬件形式实现的安全机制和服务措施。

1. 管理性安全措施

下面罗列在选择和实现过程中常见的各种管理性安全措施，罗列的顺序不考虑安全措施实施的先后顺序或逻辑关系。

1）信息安全管理和策略原则

此类安全措施包含在信息系统安全生命周期的各个阶段实施管理，以及各阶段之间保持一致性的活动与对这些活动的规范。这些安全措施在于使整个组织在信息系统生命周期中保持合适的、一致的安全目标、方针和策略。下面列出了此范围内的常见安全措施。

（1）制定组织的信息安全策略

编写含有规则、指令、惯例的书面文件，用来描述在组织内部应怎样管理资产和保护资产。在信息安全策略文件中应指明哪些信息系统资产需要管理和保护，以及对其进行管理和保护的规程。

（2）制定信息系统安全策略

对每一个信息系统制定含有规则、指令、惯例的书面文件，用来描述组织识别已有的或有必要增加的安全措施的规范，其中已有的安全措施包括计划中和正在实施的安全措施。

（3）信息安全管理

以适合本组织的制度化和规范化的活动方式对信息系统生命周期过程中的安全实施管理，并使所有的安全管理活动在组织内保持协调和一致。在这一过程管理中，信息安全委员会、信息安全官员对组织的信息安全管理活动进行协调和监督。

（4）分配责任

将组织内各层级、各部门、各岗位在信息系统安全中的责任明确地写入文件，并根据组织的部门性质制定具有可操作性和便于监督的管理规范，根据岗位特点制定具有可操作性和便于检查的操作规程，做到各类人员在安全管理中权利和义务的相对平衡。

（5）管理活动的信息安全

对所有管理业务的流程（如采购、组织内的协调、与其他组织的沟通与合作等）都应以安全的方式进行组织，提供对信息安全管理的系统性支持。

（6）确认和评估重点保护资产

对组织内与信息系统有关的资源进行识别，并评估这些资源对组织业务的价值，对那些具有关键作用和重要价值的资产予以特别关注。

（7）信息系统验收中的安全审查

在信息安全策略指导下验收信息系统，对于验收过程的每一步都要审查实现业务流程过程中的安全措施是否能提供对业务流程适当的保护等级水平。

2）遵从性检查

对信息安全措施从设计开始到报废的整个过程都要进行遵从相关的法律、法规、政策和安全策略的检查、复核和审计等活动，这是确保安全机制和服务措施有效发挥安全保护作用的约束性措施。这一方面的安全管理措施如下：

（1）遵从信息安全策略

由信息系统的安全管理官员定期检查所有用户遵从信息安全策略的情况，并组织对所有的信息系统的安全措施与信息安全设计中列出的相关的安全措施和技术标准一致性的复核。

（2）遵从法律和法规

检查信息系统运行中遵从所在国的法律和法规（如数据保护和隐私保护、软件复制、组织档案记录保护及加密技术等方面的相关立法）情况。在信息安全策略中必须保证将这种遵从性写入法律要求条款中，并确保信息系统的每项安全措施在实现时是满足这些法律要求的。

3）处理安全事件

信息系统中的每个岗位的员工都应按报告制度将发现的安全事件的有关信息和活动及时向组织的安全管理人员报告，并依照操作规程及时处理安全事件中属于本岗位职能应该做的事务。有关处理安全事件的事务如下：

（1）报告安全事件

信息系统中的每一位员工在发现安全事件发生或可能发生安全事件的有关信息（如线索、预兆）时要及时报告有关的安全管理人员。

（2）报告安全漏洞或缺陷

信息系统的使用人员一旦发现与本系统有关的任何安全漏洞或缺陷，必须立即报告给组织的信息安全管理人员。

（3）报告软件故障

信息系统的使用人员一旦发现任何的软件故障，必须立即终止正在处理的事务，同时报告信息系统管理员。

（4）管理安全事件

由组织制定对信息安全事件的管理流程，支持对安全事件的防范、检测、汇报和应急处置。管理流程包括收集、评价安全事件的信息，提出防止事件再次发生或减小再次发生造成损失的建议。

4）人员管理

关于人员的安全措施是要减少由于人员操作失误和违反安全规定（故意或无意）所造成的安全风险。这方面的安全措施如下：

（1）针对系统内员工的安全措施

务必使与信息系统有关的所有员工知道他们在信息系统安全上的作用和责任，制定员工应该遵守的与安全有关的操作规程和行为规范。在雇用前对员工进行可信性审查，如果有必要还要签订保密协议。

（2）针对临时工的安全措施

对临时工（如保安、清洁工等）及所有参观考察者进行控制。在临时工获得接触（物理或逻辑的）信息系统设施的权限之前应该让其签订保密协议。

（3）安全意识和培训

所有管理、使用、开发、维护及对信息系统设施有访问权的人员都应阅读定期发布的安全简报和材料，应该教育并使工作人员知道他们掌握的信息对组织安全的重要性，以及这些重要信息存在的脆弱性、潜在威胁和风险，以使他们理解安全措施的必要性。另外，还应对使用信息系统完成本职工作的人员进行安全培训，包括岗前培训和在岗培训，以让他们正确地使用信息设备，避免错误操作和违规操作。对于信息安全官员、信息安全管理员等关键人员，则必须进行更深入、更专业的安全知识和安全意识的培训。

(4) 严明纪律

要使信息系统所在组织的所有员工知道,(有意和无意)违反组织范围内的或具体的信息安全操作策略和行为规范以及其他必须遵守的与安全有关的合同条款、安全协议,必须承担相应的后果。

5) 与安全有关的操作事项

操作方面的安全措施是指维持信息设备及相关系统(组件)安全、稳定和可靠运行的一系列程序性的操作规定。通过执行这些规定就可以保证信息系统的安全措施发挥安全保护效能。操作上的安全管理措施与其他管理性和技术性的安全措施配合使用,可以最大限度地使安全保护措施发挥作用。这方面的安全措施如下:

(1) 配置和变更管理

配置管理的目的是操作和控制信息系统的安全运行以及系统资源的安全特性,变动管理的目的是识别信息系统发生的变更,并帮助在信息系统发生变更后选择新的安全措施。

配置和变更管理的基本安全目标就是保证信息系统处于正常的安全运行状态,并使发生的变更不至于降低安全措施的可用性和安全措施所保证的整体安全性。

(2) 维护

为了保证信息系统持续的可靠性、可用性和整体性,必须对其中的软/硬件设备进行日常性维护,要在维护规范中写明维护人员必须遵循的安全要求。维护工作外包的,应在与服务商的合同中写明维护中必须遵循的安全要求,承担维护业务的服务商必须具有相应的组织和专业队伍。

(3) 监控与安全有关的变更

对信息系统发生变更的部分及其关联的信息资源的脆弱性、面临的威胁和影响进行跟踪监控,根据监控结果进行风险评估。这些变更包括信息系统自身的变更、需要遵从的法律发生变化和信息系统所处物理环境发生的变更。

(4) 审计跟踪和日志

从规程上要求信息安全管理员和系统的操作员使用专用审计工具,并充分利用软/硬件设备(包括处理信息的设备和保护安全的设备)中已有的日志记录和审计功能(例如服务器的操作日志记录和分析工具,网络设备(路由器)中的日志信息和统计信息,防火墙中的日志记录和审计信息,应用程序中的交易处理日志信息等)对信息系统的安全状态进行跟踪。有条件的信息系统应该将系统内各种设备的日志信息和审计信息整合起来,从中挖掘出安全事件的特征模型,为"事前预警、事中控制和事后审计、追究"的安全事件管理模式提供可靠的准确信息。

对操作日志的分析审计应定期进行,以发现各种形式的未经授权的操作和违规操作行为。对日志的分析和审计还可为验证系统所配置的安全措施的有效性、证实安全措施的充分性提供额外的支持;对日志中的重复性事件进行分析,将有助于准确地识别系统的脆弱性和面临的威胁。这样的分析还可以从表面上不相关的事件中挖掘出某种模式,以更深刻地理解和认识信息系统安全要素之间的内在逻辑。

(5) 安全测试

所有的安全设备和所有的相关软件(包括操作系统、平台型软件和应用程序)必须通过国家授权的测评机构进行的安全保证水平测试。安全保证水平测试应符合在信息系统安全

策略中规定的测试标准，以判断是否达到了要求的安全保护等级。

(6) 介质控制

介质控制包含对磁带、磁盘、USB 等移动存储设备、光碟(光盘)、输出装置及其他介质的保护和控制，保护措施有物理性保护和环境保护措施；控制措施则是对这些存储介质在保存、使用和销毁的生命周期的管理规定，包括做标记、使用的日志记录、完整性验证、物理使用权和保管、使用责任的规定。

(7) 信息的彻底删除

制定对存储的机密信息进行物理性删除的规范，对于尚存有或存入过机密信息决定不再使用的存储设备制定物理性销毁的规范。保证含有机密信息的文件已被抹掉并进行了物理性覆盖，或者已被毁掉。由于计算机的删除命令并不能保证做到以上要求，需要为使用人员提供能使他们彻底删除信息的方法和工具。

(8) 分割操作特权

为了把滥用特权的风险降至最低，需要对一些操作特权(例如初始参数配置、查看审计信息等)进行分割。那些可能绕过或穿透安全措施和规避审计的操作特权以及可能使员工获得过多或超出本职所需的操作权限，必须进行分割。

(9) 控制有版权软件的使用

保证不使用复制的有版权控制的软件，并严格遵守专有软件的许可协议。

(10) 控制软件变更

对软件进行变更时必须遵从论证和报批规定，保证变更不影响正常业务的连续性和完整性，不因软件的变更而引入新的风险。需要特别提醒的是，软件变更控制仅针对软件系统，而配置和变更管理针对信息系统及其运行环境。

制定能对软件变更进行控制并使信息系统维持在期望安全等级上的完整规范，其中包括对软件变更的授权制度、变更方案的安全考虑和最终应达到的安全等级水平。

6) 业务连续性措施

制定业务连续性(包括意外事件的应急措施和失效恢复)的方案和措施，确保组织的业务，特别是关键业务流程，免于遭受重大故障或能力丧失所带来的影响，或把损害降至最低。这些措施如下：

(1) 意外事件处理策略

在识别出因信息系统资源脆弱性、系统调整和破坏行为对组织可能造成潜在的负面影响的基础上制定意外事件处理(包括意外事件的应对措施和失效恢复)策略(规则和指令)，并形成正式文档。

(2) 业务连续性计划

在业务连续性策略(流程或规范)的基础上制订业务连续性计划(包括处理意外事件和失效恢复的方案和措施)，并形成正式文档。

(3) 测试和更新

在业务连续性计划获得批准前应彻底地测试连续性计划在维持信息系统生命周期中不间断服务能力的充分性，制定一个使所有相关人员都理解这些计划的分发和培训规程。业务连续性计划必须根据系统和环境的变化进行更新，业务连续性策略也应同步进行更新。

(4) 备份

对信息系统中所有数据(控制数据、管理数据和应用业务数据,管理文档,操作系统和应用程序等系统数据)和(必要时)最小集的软/硬件系统都必须按规程进行备份。数据备份频度依照信息的重要性和业务连续性计划的规定而定,使其与信息的重要性和业务连续性计划相适应。一般信息系统的数据备份必须至少在信息系统运行环境内保存一份,并在信息系统所在建筑物以外的地方(同城或异地)保存一份;对于重要的信息系统,除在异地备份一个最小集的软/硬件系统外,还应将数据备份保存在运行环境内和信息系统所在建筑物外的同城建筑物内以及远程异地各一份。按规程定期更新和维护备份,定期维护已备份的最小集软/硬件系统,确保备份的可靠性。

7) 物理安全

物理安全措施是对信息系统软/硬件设备、子系统或组件及运行环境进行物理保护的活动的总称,物理保护形式可以是规程性的,也可以是技术性的。下列措施可用于对建筑物、安全区域、计算机房和办公场地等进行保护。这方面的安全措施如下:

(1) 环境保护

环境保护包括对建筑物的所有物理保护措施(栅栏、门禁或保安、坚固的围墙、门窗控制、视频监控等)。通过栅栏、围墙和门窗控制将信息系统进行内外物理隔离;通过对物理访问身份和权限的控制(门禁或保安)防止未经许可的人员进入安全控制区;通过视频对信息系统周边和内部重要的安全区域的异动情况实现全天候的无人值守监控。

(2) 防火

应对设备及其周围环境采取措施,以发现火灾苗头和防止火势从建筑物内或从邻近的其他建筑物蔓延过来。在存放信息系统设备的房间和地区的附近必须有火警标志,在这些设备附近和房间内外安装水栓、烟火检测装置和灭火器具,并定期检查和更新;在关键设备存放地(或区域)与外部区域之间设立火灾隔离措施,充分利用视频监控设施对火灾的发生或蔓延进行预警。

(3) 防液体/防腐蚀

关键设备附近不能存放可能发生泄漏的液体和具有腐蚀性的液体、固态材料等。

(4) 防自然灾害

信息系统的重要和关键设备必须安放在具有防洪水、防雷电的房间或建筑物内;设备自身应采取严格的接地保护措施;信息系统所在建筑物要有适度的坚固强度和抗震能力,并远离洪水泛滥地、泥石流经过区;充分利用视频监控设施对自然灾害的侵害进行预警和报警。

(5) 防盗

为所有的信息系统设备(包括便携式软/硬盘、USB 存储介质等)贴上具有唯一性的身份标记,有条件并且必要时可采用具有 GPS 功能和 RFID 识别方法的身份标识;对存储介质上的敏感信息和专有软件嵌入控制信息,阻止未授权使用直至自动销毁;将所有的设备编制成详细的资产目录。

门卫人员应对进出系统的人员、设备、材料和器具进行识别,对未经授权出入的人员或带离房间、区域或建筑物的设备材料和器具等予以阻止,并登记和追查。对存于便携式介质(如软盘、移动存储设备)上的敏感信息和专有软件应进行适当保护,以防止丢失或被盗。

(6) 电源和空调保障

使用不间断电源系统(UPS)在断电时作为应急供电设施,确保信息设备安全和对系统内不允许意外终止的进程实现紧急的系统关闭,并完成对业务数据的存储及备份。UPS 维持电力的时间长度根据信息系统的重要程度决定;在必要的地方可用 UPS 作为信息系统或其中某些子系统或组件的后备电源。

使用具有温/湿度控制和空气净化功能的空调系统,对信息系统的软/硬件设备运行(含存储)场所进行保护,前者保护设备不因环境温度变化而降低或丧失性能,后者保护设备免于粉尘的危害。

(7) 电缆保护

采取措施防止电源线和通信数据传输线被物理(人为地或自然的)截断、损伤和破坏。所采取的保护措施包括技术性的物理措施,例如采用坚固耐损的材料,紧固地安装并加保护外套等;管理性的措施,例如在线缆经过的地方进行明显标示,加强法制宣传,经常性巡视等;法律性的措施,例如对无意的轻微的人为损坏依法追偿,对有意的人为破坏或无意的但重大的人为破坏追究刑事责任。在通信电缆经过的公共场所的地方要防止电缆被搭接。

2. 技术性安全措施

1) 识别和鉴别

识别是将某一实体从一群实体中区别出来的过程。鉴别是对实体所声称身份的真实性进行确定。一般来说,识别和鉴别这两个过程是连续进行的,其中识别与身份标识有关,鉴别则需要实体的附加信息。在计算机信息系统中对用户的识别和鉴别只有通过技术的方法才能进行。以下是完成识别与鉴别的一些措施。

(1) 通过使用实体知道的信息进行识别与鉴别

口令(即 PASSWORD,通行字)是用于鉴别的最典型的形式,是验证用户身份真实性的依据。在网络环境中使用的口令一般由系统管理员分配,或系统授权用户自己编制后存入系统。当计算机不与网络连接时,进入计算机的口令完全由用户自己确定。在网络信息系统中,与口令有关的操作应受到规程的严格约束。

口令应不少于 6 个字符,一般由数字和字母混编,最好包含数字、大小写字母和特殊字符,并定期更新。

用户自己的口令不得泄露给其他人,口令副本应像保存密钥一样保存;存放在信息系统中的口令表必须经过加密处理,且只有系统管理员或获得特别授权的人才能读取。当使用人员忘记口令时或遗失口令副本时,必须履行报批手续,才能由系统管理员重新分配。

口令鉴别是常用的身份鉴别方式,也可以使用密码方法和鉴别协议对用户身份进行远程识别与鉴别,以增强安全性。

(2) 通过用户持有物进行识别与鉴别

其典型例子是用户利用具有存储功能的各种智能卡或令牌进行识别和鉴别。具有存储功能的智能卡最常见的应用就是信用卡背面的磁条或 IC 卡信息。用户持有的卡或令牌是身份的标识,用户的口令则是确认用户真实性的依据。用户所持有的卡或令牌一旦丢失,需要立即报告,并予以注销。

(3) 通过用户自身的特征信息进行识别与鉴别

用户的生物特征(如指纹、手掌形状、视网膜、脸形和声音等)信息具有相当高的唯一性,

可以用来识别和鉴别用户的身份。相关的生物特征信息必须安全地存储在智能卡或系统中。其中,生物特征是用户的标识,而生物特征信息是确认用户身份真实性的依据。

2）访问控制和日志

访问控制通过在系统中的通信连接或数据流程中设置某些判断或约束条件对用户访问系统资源进行限制或控制。其作用是限制或控制系统内外用户对信息体、计算机、网络、应用程序、文件和程序的访问。访问控制一般利用嵌入在某个子系统或组件的一段计算机程序或模块程序即可实现,也可以使用硬件或附加设备来实现。

一般地,访问控制前必须对用户的身份利用识别和鉴别措施予以确认。

访问控制列表是信息系统中常见的用于说明访问控制约束条件或前置条件的一个序列。与访问控制有关的安全措施如下：

(1) 访问控制策略

每个系统或子系统都要制定访问系统内资源的控制策略,访问控制策略以一组有序的规则组成,清楚地说明哪些用户具备哪些条件才能访问哪些资源,其中的条件包括对用户的身份和操作权限的规定。此外,访问控制策略还需说明访问控制属于缺省(默认)禁止(除了允许的一律禁止)模式,类似于红名单控制方式；还是属于缺省(默认)允许(除了禁止的一律允许)模式,类似于黑名单控制方式。

对访问控制模式的选取应该考虑组织获得安全的方式(开放式或限制式)和文化特点,以在满足业务安全的同时让用户易于接受。

(2) 用户对计算机的访问

对计算机的访问控制的主要目的在于防止未经授权使用计算机资源。对每个已获授权的用户的身份进行确认和核实是必要的。

(3) 用户对数据、公共信息服务和应用软件的访问

控制计算机或网络中的数据、公共信息服务和应用软件的使用。控制这些访问的方法一是在计算机和提供公共信息服务的设备(例如服务器和服务器群)的入口处安装防火墙一类的隔离控制系统,二是在各类应用程序(例如业务软件、信息服务软件)中嵌入访问控制模块。访问控制可以是基于角色、基于任务的,也可以是面向资源和面向用户的,等等。

(4) 对访问控制措施进行检查和更新

对访问控制措施要进行定期检查。如果现有的访问控制机制已不能满足安全或业务需要,就要进行扩充或更新控制功能。对具有优先访问权用户的访问情况应进行更频繁的检查,以防止访问权力被滥用。如果对某些信息系统资源的访问已不再有必要,应及时收回访问权。

(5) 日志记录

对信息系统进行的所有访问活动都应该记录到日志中,并对日志进行定期的检查和分析,这包括对系统成功和不成功的登录、对访问的数据的记录、对访问的系统资源的记录等。另外,错误的操作也应该被记录下来,并进行定期检查。对访问行为的记录数据应遵从有关数据保护和隐私保护的法律,例如这些与访问有关的数据仅能在有限的时期内保存,并且仅能用来查找安全违规问题,不可外泄,或被审计人员以外的人员查看(除非获得特别授权)。

3）防护病毒与恶意代码

病毒和恶意代码可以通过外部接口(例如与软/硬盘、移动存储设备、网络连接等的接

口)和木马程序引入系统。病毒和恶意程序对任何信息系统造成的现实的和潜在的风险都很难识别并控制,如果不采取有效的安全措施,一般只有在恶意代码发作并造成损害后才能发现它。与恶意代码有关的程序形式如下:

- 特洛伊木马(Trojan Horse)程序(一种内含病毒和恶意代码、行为隐蔽的程序);
- 病毒(一种具有自我复制、传播能力的有害程序);
- 恶意程序(一种对信息系统及其资源具有特定破坏能力的小型程序,常常隐藏在木马程序中或寄生在可执行程序中)。

其中,木马程序是运载和隐藏病毒和恶意代码的工具之一,对信息系统造成危害的是病毒和恶意代码程序。

传播病毒和恶意代码的途径如下:

- 软盘复制;
- 访问便携式存储介质;
- 电子邮件传播;
- 网络传播;
- 文件或网页内容下载;等等。

预防、阻止病毒和恶意代码的安全措施如下:

(1) 扫描

使用病毒、恶意代码和木马扫描软件,对系统内已有的和新运行的程序、存储区域进行定期扫描,检测出已知特征或疑似特征的病毒、恶意代码和木马,并予以清除或杀灭;对以任何形式来自系统外部(软盘复制、USB 接入、网页下载、邮件传递等)的数据、文档、程序、表格等进行扫描,检测出携带有已知特征和疑似特征病毒、恶意代码和木马程序的任何数据和程序,未经扫描不得进入系统。

(2) 检测

对病毒、恶意代码和木马的检测除利用扫描工具外,还有两种方法可以尝试。一是在系统内采用完整性检测方法,检测出系统数据的变化,从而进一步分析和判断引起变化的原因,为确定病毒和木马程序提供线索;第二种方法是利用专门工具对病毒、恶意代码和木马进行深度检测,这些检测工具可能是专门针对木马的,可能只是针对病毒的,也可能只是针对恶意代码的。它们的共同特点是不如扫描工具的检测范围大,但却具有更深入的、细粒度的检测能力,有的还有不同程度的数据挖掘和逻辑推理能力。这些检测工具除对检测出的异常数据和关联的纵向(与时间相关)、横向(与资源分布有关)数据具有较强的数据挖掘能力外,还具有更完整、更专业的特征数据库,有利于得出更精细、准确的检测结论或线索。

4) 网络安全管理

网络安全管理的内容包括对网络的规划、配置、隔离、监控、检测等。对网络进行正确的隔离、配置和监控是减少风险的有效手段。具体安全措施如下:

(1) 网络规划

为了保证组织业务系统可靠运行和具有足够的网络容量,必须根据组织的业务现实对网络系统的结构及其安全、带宽、存储容量、交换设备性能做出具有一定冗余并可扩容的规划。

（2）网络配置

网络配置包括网络结构参数配置、边界设置、带宽分配、存储容量管理和交换设备选配等。

网络结构指组织的局域网或内联网内部的连接，与外部网络的连接，以及组织员工远程接入的安排与布局，其中内部结构即内部子网络或虚拟局域网（VLAN）的布局，内部子网和VLAN可在原有的物理布线和交换设备的基础上配置，其边界由配置参数决定，可在内部子网加配安全网关和加密设备；外部结构指组织的内部网与外部网络连接的线缆和交换设备布局，其边界在路由器或交换机的外侧，必要时可加配防火墙、接入的鉴别设备或传输的加密设备等。

网络带宽和存储容量的分配根据组织业务和管理需求分配到各个子网和网络设备。

交换设备选配指对内部交换设备和与外部网络的交换设备的选配，主要考虑其交换性能，包括交换接入/出容量、交换速度和带宽等参数。

网络参数的合理配置对网络的运行性能和稳定性极为重要。

（3）网络隔离

网络隔离包括网络中的内部子网络之间的隔离和与外部网络连接的隔离。前者指在网络上将处理不同业务的主机和网络资源分别划分为若干子网络，形成相应的业务管理区域（一般称为安全域），然后将这些业务区域在逻辑上或物理上保持相互隔离，以方便管理和提高安全性；后者根据组织的网络与外界网络连接的控制需要分为逻辑隔离（一般以路由器或防火墙、安全网关为边界）和物理隔离（一般以网闸或数据摆渡设备为边界），隔离方式依对连接进行控制的需要而定。

（4）网络监管

利用网络扫描工具（一种计算机网络系统脆弱性或缺陷识别的软件包）定期对网络配置中的弱点或缺陷进行扫描识别，为网络安全措施的选择或调整提供参考。根据所识别的网络系统脆弱性或缺陷，实时地对系统的脆弱性或漏洞安装加固或补丁程序，或更新网络版和主机版防病毒软件。网络扫描工具本身也应随时更新。

（5）入侵检测

入侵检测一般在组织的网络与外部网络连接的边界处配置，也有在大型网络中子网络之间的边界处或在公共访问资源集中的区域边界处配置的。入侵检测的作用是辅助网络管理人员识别未经许可的非法或越权访问的入侵行为。入侵检测设备可以是一个以旁路方式并接在网络边界处独立运行的系统，也可以嵌入在防火墙系统中作为一个功能模块参与到对连接进程的识别中。入侵检测的理想模式是将检测结果与防火墙等隔离控制设备实现联动。

迄今为止，在入侵检测设备的实际应用中存在一个共同的问题，就是几乎所有的入侵检测结果的误报率都较高，有的入侵检测设备的误报率甚至高到超过了管理人员的容忍限度而影响对其的使用。

5）加密技术

使用加密技术保护信息系统的数据存储和传输过程的安全在信息系统安全中是一种较为普遍的做法。使用加密技术可对信息系统的数据在存储和传输过程的若干安全属性实现保护，分别如下：

（1）数据机密性

当存储或传输的信息对机密性保护要求较高时，可在物理层、链路层、网络层、传输层和应用层（主要是保护各类数据）中选择在一层或多层进行加密，实现对数据的保护。数据机密性表现为对数据的存在性、不可获取性和不可理解性的维护，加密技术可以从这 3 个方面保护其数据的机密性。在使用加密措施时应考虑以下方面：

- 遵从国家对密码技术和设备使用及管理的法律和法规；
- 密钥管理本身的安全问题；
- 保持加密机制与所需要的保护等级之间的适应性，不可盲目追求多层加密措施或高强度加密措施。

（2）数据完整性

当存储或传输的信息对完整性要求较高时，可使用散列算法、数字签名技术等密码技术措施来保护存储或传输信息的完整性。完整性安全措施（如 Message Authentication Code，MAC，即消息鉴别码）可防止对被保护信息进行有意或无意的改动、增减、删除和重放等攻击。数字签名技术措施不仅能为消息提供类似的完整性保护，而且具有抗抵赖的能力，即对信息的来源与信息的发送方的不可否认。在使用数字签名技术或其他完整性安全措施时应考虑以下方面：

- 遵从国家法律和法规约束；
- 密钥管理本身的安全。

（3）抗抵赖

抗抵赖措施指对信息的发送、传输、提交、交付和接收等行为，时间以及信息内容进行确认的特性，以防止信息的发送者和接收者对已操作过的行为以及对信息修改的结果进行否认。抗抵赖的安全特性可通过数字签名技术实现。

（4）数据真实性

当对数据真实性的要求非常高时，应使用数字签名来验证数据的真实性，以及数据是不是特定人员发来的。

（5）密钥管理

密钥管理包括对密钥和加密过程信息有关的管理活动和技术机制的组织与规程等方面的内容。密钥管理的目标是实现对密钥及相关信息的安全管理。密钥管理活动包括密钥材料的产生，密钥的生成、存储、分发、安装、注册、注销、存档、更换和销毁。合理的密钥管理体系除需实现与密钥有关的管理活动外，还必须具有对密钥管理系统及其数据的机密性、完整性和可用性保护的能力。

5.4.3.3　选择基线安全措施

下面的方法可用于选择适合于保护信息系统安全的安全技术措施。

首先是将组织可选用的组合的安全措施集适当地应用于所考虑的信息系统。由于它们具有对某一类信息系统安全保护的普遍适用性，这类安全措施集总是作为优先考虑的对象。进一步说，由于它们是通过组织的安全性分析和规程引入的，所以很多安全措施的执行成本并不高。有关这些安全措施选择的细节将在“可普遍应用的安全措施”中进行讨论。

然后是进一步考虑信息系统的具体类型和特点。有关这些安全措施选择的细节将在“具体的安全措施”中进行讨论。

当然，对于一个信息系统来说，可能某个或多个组合的安全措施集或某些具体的安全措施都没有必要采用，例如对信息的接收者或发送者来说并不需要保密，或完整性保护要求也不高，那就没有必要使用密码技术；还有一些类别的安全措施只有在获得进一步的风险评估后才能确定其是否为最恰当的选择。

如果要对安全措施的适用性做更加准确的判断，必须根据风险评估的输出数据做更详细的分析。

如果安全措施是根据不同的准则选择的，则应该对最后准备实现的一套安全措施进行仔细的搭配，并核实按不同准则做出的选择之间是否存在冲突或功能抵消的情况。

在“基线”安全模式确定之前，可考察其他已做过基线保护的同类信息系统的安全状况以作为借鉴和参考，并识别与其他信息系统之间的细微差异及这些差异可能产生的风险，评估风险的可控性。

在选择安全措施时，另一种无须进行详细分析的情况是使用针对具体应用领域的专用的“基线”模式，例如现有的电信领域、医疗保健领域、银行业领域和其他专业性很强的领域的“基线”安全模式手册就可以直接引入相应的信息系统领域指导对安全措施的选择。在使用这些手册时，可以把现有或计划中的安全措施与手册上推荐的安全措施进行对照。在最终决定要执行哪些安全措施之前，要仔细考虑安全需求和安全保护重点。

1. 可普遍应用的安全措施

可普遍应用的安全措施如下：

- 信息安全管理策略；
- 遵从性检查；
- 事件处理规程；
- 人员安全管理规程；
- 操作规程；
- 业务连续性计划；
- 物理安全措施。

这些类别的信息安全措施是成功实现信息系统保护体系的基础，是信息安全保障的最低要求，其重要性在任何时候都不能低估。这些安全措施与下面要介绍的技术性更强的具体安全措施之间的协调也非常重要。

当然，可能还有许多其他的安全措施在很多信息系统中也是应该使用的，但在具体选择时却要依具体情况而定，例如为网络提供访问控制的安全措施就不同于为单机提供访问控制的安全措施，不仅在控制力度上不同，而且控制的方式也可能不同。当从可普遍应用的安全措施中选择某些安全措施时，应该考虑组织的规模及其安全需求，例如对于安全策略类中的安全措施，一个小规模组织的小型信息系统就没有必要也没有相应的人力资源来建立信息安全委员会，可以让相应职能的岗位人员兼任相应职位。因此，在选用时，应对安全措施所具备的基本功能和效力与信息系统的实际需求进行综合比较。

2. 具体的安全措施

信息系统的安全保护体系除选择可普遍应用的安全措施外，还要根据信息系统的类型和实际情况选择其他一些具体的安全措施，这样才能满足组织对信息安全的整体要求。判断选择安全措施合理性和充分性的原则在数学上表述为同时满足必要条件和充分条件，其

中普遍性安全措施是必要条件，根据系统实际情况选择的个性化安全措施属于充分条件。在实际工作中，选择满足信息系统安全需求的充分条件是安全措施选择的核心任务。

表 5.3 给出了怎样为信息系统选择具体的安全措施的示例。标记为“√”的选项代表正常情况下必须实施的安全措施；标记为“(√)”的选项代表在某些情况下有必要实施的安全措施；标记为“—”的选项代表不需要采取安全措施。对安全措施的选择过程并没有到此结束，还要进一步考虑对安全措施的功能性描述，如果有必要，应该从有关的参考资料中获取有关安全措施的进一步的信息。

表 5.3　特定安全措施的选择

	独立的工作站	联网的工作站(不共享资源的客户机)	联网的服务器或联网且共享资源的工作站
识别与鉴别			
通过用户所知道的信息进行识别与鉴别	√	√	√
通过用户持有的东西进行的识别与鉴别	—	(√)	√
通过用户自身的特性进行的识别与鉴别	—	—	(√)
权限控制和审计			
使用权限控制策略	—	—	√
用户对计算机的使用权	√	√	(√)
用户对数据、服务器和应用软件的使用权	√	√	(√)
对使用权进行检查和更新	—	—	(√)
审计日志	√	√	√
防护恶意代码			
扫描装置	√	√	√
完整性检测(工具)	√	√	√
移动存储介质的传递控制	√	√	√
规程方面的安全措施	—	—	√
网络管理			
操作性规程	√	√	√
系统规划	—	—	√
网络配置	—	—	√
网络分离	—	—	√
网络监控	—	—	√
入侵检测	—	√	√
密码技术			
维护数据机密性	(√)	(√)	(√)
维护数据完整性	(√)	(√)	(√)
抗抵赖	—	(√)	√
数据真实性	—	(√)	√
密钥管理	—	(√)	√

5.4.3.4 根据保护重点和威胁选择安全措施

根据安全保护重点和面对的威胁选择安全措施时，首先要识别并评估安全保护重点的价值，针对每一个信息系统资源保护重点列出所面临的威胁，然后针对每一个威胁列出保护点在机密性、完整性、可用性和可确认性方面的安全需求，据此选择能满足安全需求的安全措施，并保证安全措施的功能和效力对抗威胁的充分性。

1. 评估安全保护重点

为了合理地选择适当的安全措施，首先要了解支持组织业务运营的信息系统资源中那些本身价值很大和能力丧失或降低后造成的损失很大的资源，从中识别出安全保护重点，根据这些资源的脆弱性程度和面对的威胁强度评估安全风险，导出可应对风险的安全需求，在此基础上恰当地选择能满足安全需求的安全措施。如果需要高保护强度的资源点分布复杂，则应根据详细风险分析情况来选择安全措施。对于具体需要保护这些重点资源的哪一个或哪几个安全特性(包括机密性、完整性、可用性等)，应根据风险分析结果来确定。

重点保护对象应包括信息系统本身、由信息系统存储或处理的信息、由信息系统完成或支持的业务流程。信息系统的不同部分或由信息系统存储和处理的信息的不同部分可能对应不同的安全特性，需要重点保护。把安全保护重点和保护重点中需要保护的安全特性与资产直接联系而建立对应关系非常重要，因为这样可以增强所选择安全措施与保护对象的针对性。因此这里的安全保护重点应明确地说明需要重点保护的资源点(例如某个数据存储区域或某个信息体)及其需要重点保护的安全特性(例如数据存储区域或某个信息体的机密性、完整性、可用性、可控性等)。

进一步，通过对管理缺失、不当或信息系统资源的漏洞给业务造成损失的严重性(是严重损失、较小损失还是不会造成损失)的具体分析，就可以对安全保护重点做出准确的评估。例如，如果一个组织机构的投标信息在信息系统上进行处理时被有意无意地未授权泄露，那么可能会使项目招标活动面临失控，给该组织造成巨大的经济损失或社会信誉损失，因此就要求对这类信息在各个处理环节进行严格的机密性和完整性保护；相反，如果本是已经公开的信息在信息系统上进行处理，那么未授权的泄露并不会给公司造成实际的损失，那么对这类信息就无须进行机密性保护，但应进行完整性保护。所以信息系统资源在不同的业务安全目标情况下同样存在的脆弱性在面对同样的威胁时所产生损失的严重程度可能完全不同，所需的安全保护需求的差别很大。

如果信息系统处理多种类型的信息，那么就应根据信息的种类分别评估。对信息系统进行的保护应该保证对所有种类的信息的安全需求都是足够的和均衡的。这时，如果某些信息需要较高要求的安全，那么应对其适当加大保护。如果系统中只有很少的信息涉及较高的安全要求，可考虑把这些信息集中起来移到一个子系统或一个小的区域中单独给予高强度的安全保护，避免由于保护个别信息而提高整个系统的保护力度。当然，前提是这样做不会导致业务流程的冲突。

当可能发生的机密性、完整性、可用性、可确认性和真实性等安全特性降低或丧失只会造成可以忍受的损失时，选择某类基线安全措施就能为所涉及信息系统提供足够的保护。如果经评估会造成严重的或不可接受的损失，就应考虑增加额外的安全措施，必要时采用详细风险分析方法来确定安全措施的选择。

下面对一些常见安全特性的丧失可能导致的后果分别给予示例性说明：

1）丧失机密性

资产机密性的（有意或无意）丧失会导致：

- 组织或其信息系统失去公众的信任，或损害组织的公共形象；
- 引起法律纠纷或责任，包括由违反与数据保护有关的法律所引起的问题；
- 由于组织内部信息的（有意无意地）不适当泄露引起社会动荡；
- 个人隐私受到侵犯；
- 直接或间接的经济损失；等等。

上述示例性说明只是列举，不是概括，更不是穷举，本小节后面类似地方的说明与此相同。

根据对这些列举（不限于这些列举）示例的具体理解可判定丧失机密性会造成的损失的严重程度是严重、一般还是无关紧要。

2）丧失完整性

资产完整性的（有意或无意）丧失会导致：

- 不完整的信息导致决策发生错误；
- 对内信息不可用；
- 对外信息错乱，损坏组织形象和信誉，丧失公众信任或市场份额，或造成社会恐慌；
- 业务管理职能出现混乱；
- 现实的和潜在的经济损失；
- 引起法律纠纷和责任，除承担严重违反国家法律的责任外，甚至可能导致巨大的社会不良后果或巨额经济赔偿；等等。

根据对此类列举（不限于这些列举）示例的具体理解可判定丧失完整性会造成的损失的严重程度是严重、一般还是无关紧要。

3）丧失可用性

应用软件可用性或信息可用性的（有意或无意）丧失将引发一系列问题，导致：

- 无法执行管理业务，或无法提供组织承诺的信息服务；
- 组织或其信息系统失去公众的信任，或损害组织的公共形象；
- 引发各种合同纠纷或巨额赔偿；
- 直接或间接的经济损失；
- 法律责任，包括由违反与数据保护有关的法律所引起的以及因违反合同的最后期限规定所引起的责任；
- 巨大的恢复成本；等等。

应该注意的是，丧失可用性所造成的损失一般会因可用性丧失时间的长短不同而有很大的差别。所以应考虑在不同时段内可用性的丧失会带来的各种损失，并评估每个时段中丧失可用性可能造成损失的严重性，并以此制订相应的应急恢复计划。

根据对以上列举（不限于这些列举）示例的具体理解可判定丧失可用性造成损失的严重程度是严重、一般还是无关紧要。

4）丧失可确认性

系统用户及其行为的可确认性的丧失可能导致：

- 用户对系统进行违规或越权操作；

- 发生非真实用户的欺骗行为；
- 为商业间谍留下入侵系统的机会；
- 无法跟踪到操作主体及其行为；
- 法律责任，包括违反与操作行为有关的法律所引起的责任，由于不能确认真实责任者，组织必须承担不该承担的责任；等等。

根据对以上列举（不限于这些列举）示例的具体理解可判定丧失可确认性会造成损失的严重程度是严重、一般，还是无关紧要。

5）丧失真实性

数据和消息来源真实性的丧失会造成无法确定消息的真实来源或消息的真实性，不管这些数据和消息是被人使用还是被系统使用，都会产生不可预测的后果。尤其在分布式系统中，这类问题更为突出。丧失真实性会导致：

- 发生欺骗行为；
- 不真实的信息会误导用户或系统做出错误操作和判断；
- 无法确认外部人员对系统进行的操作；
- 为商业间谍留下可利用的漏洞；
- 法律责任，包括违反与操作规范有关的法律引起的责任。

根据对以上列举（不限于这些列举）示例的具体理解可判定丧失真实性会造成损失的严重程度是严重、一般还是无关紧要。

2. 维护机密性的安全措施

本节列举可能会危及机密性的威胁形式和维护机密性的安全措施，包括从不知其存在性、不可访问性和不可理解性 3 个方面予以描述，其中所说的机密性信息与机密信息的概念是不同的，前者说的是具有机密性属性的信息，后者说的是按照国家保密规范所确定的涉及国家秘密的某一个等级的信息，不过适用于对机密性信息的保护措施是保护机密信息的基本的或最低要求的保护措施。

1）防窃听

未授权访问机密性或敏感信息的手段之一就是窃听，例如利用无线窃听电磁泄露或通过线缆通信的数据，下面介绍相应的安全措施。

- 物理性的安全措施：通过对房间、墙壁、建筑物或传输线路等采用电磁屏蔽措施可使基于电磁波窃听的行为无法进行或代价过高；另外一种方式是进行电磁干扰，增强其窃听的难度；对网络布线采用屏蔽或双绞线缆，有条件的地方尽量采用光纤电缆，这对防窃听也有一定的帮助。
- 通过策略防范：对敏感信息或机密性信息可在约定时间、地址和经过路径等方式下传输和交换。
- 技术保护：防窃听的常用且有效的方法是加密存储和加密传输。

2）防恶意代码

针对在系统内植入代理程序监听或直接窃取机密性信息的威胁，可采取的安全措施如下：

- 对潜入或植入信息系统的代理程序（恶意代码）加强检测并予以清除，其他安全措施见“技术性安全措施”中的第 3 小点。

- 预警和事件处理：及时报告异常事件能限制恶意代码攻击，或降低攻击的成功率，或降低所造成的损失。

3）防口令猜测

针对口令猜测的威胁，相应的安全措施如下：

- 增加口令字的复杂度，采用数字和大小写字母混编，必要时可加入特殊字符；
- 用单向加密数字作为用户的口令字，然后在服务器端将口令还原；
- 增加口令字的长度；
- 定期更新口令；
- 采用一次一口令的方案。

4）防用户身份冒充

针对冒用用户身份的威胁，相应的安全措施如下。

- 识别与鉴别：采用用户记住的信息、所持有的东西或固有特征信息实现识别与鉴别，必要时组合使用这 3 种识别与鉴别方式，加大冒充身份的难度。
- 访问控制：访问控制虽然不能区分合法使用者和未授权冒充使用者，但是可在访问控制机制中附加判定条件（例如基于角色的权限、基于对象的访问权限等）阻止冒充身份者访问机密性信息。
- 加密保护机密性信息：对需要保护的机密性信息采用密码技术保护，即使冒用身份者访问到机密性信息，由于不持有解密的密钥，也无法获得或理解机密信息。

5）防消息的错误路由

消息的错误路由指故意或意外地将消息引导到错误的传输方向或不期望的接收地。面对这类威胁，相应的安全措施如下。

- 网络管理：确保路由表不被未授权修改。
- 签名保护：采用签名技术，使非法接收信息者无法还原机密性信息。
- 对机密性数据加密保护：一旦出现机密性信息被引导到不期望的接收者，由于不期望的接收者不持有解密信息的密钥，因此无法获得或理解机密信息。

6）防盗

含有机密性信息的系统组件或存储介质一旦被盗，可能直接导致机密性信息的外泄和密码系统被破译，后果不可预料。面对此类风险，相应的安全措施如下。

- 物理安全措施：通过强化物理保护措施（例如多重门禁）对存放机密信息的系统设备的建筑物、区域和房间的访问进行控制。
- 强化人员管理：对进/出存放机密性信息场所的人员实行许可制度。信息系统工作人员实行 ID 智能卡门禁出入制度；合同合作人员实行有效期临时出入证制度；外访和参观人员实行有人陪同和现场监控的登记制度；实行所有人员未经许可不得将信息系统组件或存储介质携带出门的制度，经批准凭条携带物品出门者必须登记在案。合同合作人员在规定期限内临时进入存放机密性信息场所，必须签订保密协议。
- 加密保护机密信息：对存放在信息系统内和便携式存储介质中的机密性信息采用密码技术加密保护。
- 介质控制：对任何含有机密性信息的介质制定拥有、管理、保管和使用的控制规范。

- 视频监控：对存放机密性信息的场所以及建筑物内的关键部位安装视频监控系统。
- 应急处理：一旦发现涉及存有机密性信息的设备、组件和介质等被盗或丢失，应立即启动应急机制。应急机制包括立即报警，维持现场，追踪、锁定、控制嫌疑人员，更换密码系统，等等。

7）防未授权使用计算机、数据、服务和应用软件

对计算机、数据、服务和应用软件的未授权使用可直接或间接导致信息的机密性丢失。面对此类风险，采用的安全措施如下。

- 身份鉴别和权限管理：加强对使用计算机、数据、服务和应用软件的用户身份鉴别；对访问权限实行更细粒度的分割，有条件的地方配置 PMI（权限管理基础设施）系统，强化对用户访问信息系统资源的限定。
- 访问控制：除附加物理访问控制措施外，在逻辑访问控制机制中附加判定条件（例如基于角色的权限、基于对象的访问权限等）阻止未授权访问机密性信息。
- 网络分割：将不同业务、不同用户群、不同信息资源等采用物理的和逻辑的方法对网络进行分割，增加未授权访问的难度。
- 存储介质控制：在计算机上安装移动存储介质（特别是 USB）使用控制系统。在通过计算机使用这类存储介质存取信息时，对存储介质的来源和合法性、持有人的可信度、介质内信息的传播范围等进行识别控制，阻止任何形式的未授权使用。
- 加密保护机密性数据：对系统中可能面临未授权访问机密性信息的威胁采用密码技术加密保护机密性信息，即使机密性信息被未授权访问，无解密密钥也不能获得或理解机密信息。

8）防对存储介质的未授权访问

任何对存储介质的未授权访问及使用都可能会危及个人隐私及组织信息系统资源的机密性。防止未授权访问介质的安全措施如下。

- 物理安全：对集中保管涉密存储介质的场所实行严格的门禁措施，必要时安装视频监控系统；个人所持有的含有机密性信息的介质应保存在保密场所；个人持有的存储介质（重点是 U 盘）不得随意带在身上，载有个人隐私的介质应保管在个人认为保密的地方。
- 管理：含有机密性信息的存储介质的分发和借、还必须进行登记；分配给个人专用的涉密介质不得带离保密场所，确需带离保密场所的必须报经批准并登记；涉密介质在涉密系统中的使用必须登记，说明其用途和去向；个人保管的存储介质未经他人许可不得在他人计算机上存取信息。
- 必要时在计算机上安装存储介质使用控制系统，对通过存储介质存取机密性信息进行识别和控制。
- 加密保护机密性信息：通过密码技术对介质上的机密性信息提供最后的保护。

上面描述了大量的保护信息资产机密性的技术性措施，从中可以发现，有的技术措施可以从几个方面保护信息资产的机密性，例如加密控制措施如配置得当，既可从信息资产的不可访问性保护其机密性，又可从信息资产的不可理解性方面保护其机密性；另一方面有的地方则需要多种技术措施联合保护，例如为了保护特别敏感或重要的信息的机密性可能要求在存储、传输的多个方面进行加密和访问控制的保护。

3. 维护完整性的安全措施

本节列举可能危及数据完整性的威胁及相应的安全措施。

1）防存储介质损伤

存储介质发生霉变、机械变形和裂纹等情况，会危及存储于其上的数据的完整性。面对此类风险，相应的安全措施如下。

- 控制存储环境：存储介质的存放场所应保持恒温、恒湿和空气净化，存储介质上不得负重，定期检查存储介质的物理形态安全。
- 备份：存储介质上的所有文件、业务数据都应该进行完整备份，并定期更新备份。

2）防未授权访问

任何未授权访问存储介质的行为都可能导致对其信息的修改，破坏信息的完整性。面对此类风险，采取的安全措施如下。

- 鉴别与权限：使用身份鉴别技术识别并限定访问存储介质的主体，防止身份假冒，进一步核定访问主体对存储介质的访问权限，阻止未授权或越权访问存储介质。
- 访问控制：在访问控制机制中附加判断条件（例如基于角色的权限、基于对象的访问权限等），阻止越权访问存储介质。
- 审计与监控：通过主机审计与监控系统发现用户未授权访问存储介质的尝试或案例，发出警告并采取补救措施。
- 检测恶意代码：定期检测可能潜入系统的恶意代码，并予以清除。

3）防数据篡改

对存储介质上的数据进行的任何形式的未授权修改、增减、删除和重放都是对数据完整性的破坏，导致的后果是不可预料的。面对此类风险，采用的安全措施如下。

- 加密保护：通过带恢复功能的对称加密技术对被保护数据加密，实现对完整性破坏的检测，并恢复被修改的数据。
- 数字签名保护：通过带恢复功能的数字签名技术给被保护数据附加一个密码检验值，识别被保护数据遭到完整性破坏的情况，并恢复被破坏的数据。

从上述列举的完整性保护措施中可以发现，有很多措施与保护机密性的措施相似或相同。事实上，有一些技术措施的确能在保护机密性的同时也保护完整性，同样，有一些技术措施在保护完整性的同时也保护了机密性。在下面的叙述中存在类似情况。

4. 维护可用性的安全措施

可能危及可用性的威胁和相应的安全措施如下。

1）防毁坏性破坏

毁坏性破坏指的是通过物理的或逻辑的方法使信息系统及其组件和数据不能保持其物理形态或逻辑形态的完整性，导致信息系统（或组件）瘫痪、丢失或无法提供信息服务。面对此类风险，采用的相应安全措施如下。

- 法律性威慑：制定严格的操作规章制度，让所有的员工都意识到必须审慎操作，如果毁坏了信息或系统（或组件），则无论是故意的还是无意的，必须受到纪律或法律的惩处。
- 防盗窃：信息系统的所有运行部件（包括软/硬件系统、组件）必须采用严格的物理保护和保安措施以及严格的登记制度，并在关键的场所加装视频监控系统。

- 防丢失：对信息系统的所有部(器)件实行明细登记，在系统进行例行性检查和维护后必须逐一核对系统部件，确保信息系统维持正常运行所需的部件是完整的。
- 备份：系统中所有的文件、业务数据都应该制作备份，必要时对信息系统做最小集软/硬件的系统性备份。

2）防存储介质不可用

存储介质发生霉变、机械变形和裂纹等情况会危及存储于其上的数据的完整性，从而导致数据直接不可用，或被引用时不可用。面对此类风险，安全措施如下。

- 控制存储环境：存储介质的存放场所应保持恒温、恒湿和空气净化，存储介质上不得负重，定期检查存储介质的物理形态安全。
- 备份：存储介质上的所有文件、业务数据都应该进行完整备份，并定期更新备份。

3）防通信设备及服务方面的故障

通信设备及服务故障会危及数据交换和传输的可用性，轻则影响信息系统的运行效能，降低服务质量，重则使信息系统瘫痪或不能提供服务。面对此类风险，除设计时要有预案(例如带宽冗余、关键设备的冷热备份)外，故障出现后应分析原因，采取相应的安全措施。

- 启动紧急预案：系统出现故障或故障苗头时，应按应急计划的规范有组织地迅速查找并锁定故障点，封闭故障点；若判断关键设备(例如骨干网络交换设备)出现故障，必须立即启动紧急预案；凡是有冷备份的设备应立即切换到运行状态。
- 冗余与备份：信息交换设备和存储设备均应适当备份，投入运行的设备的性能也要有适度冗余，以降低超载发生信息阻塞的可能性。在设计时，要根据最大可接受的停工时间确定备用设备性能和部署。在任何时候，系统及关键设备的配置数据都应进行备份，以应紧急之需。
- 网络管理：网络管理人员要利用网络管理工具加强对通信网络基础设施运行情况的监视，及时发现人为或设备缺陷引起的事故苗头，并通过资源调度和调整配置参数解决问题；密切监视来自内外的通过网络破坏通信网络基础设施的先兆和企图，一旦发现可疑迹象，要采取果断措施(包括预警和跟踪)。
- 保护线缆：对铺设的线缆和接头要采用坚固的物理措施构造保护层，达到抗击自然灾害和人为破坏的合适水平；在线缆集中连接等关键部位加装坚固的保护装置，必要时安装视频监控系统；定期检查和修复存在隐患的线缆及保护层。
- 抗抵赖：对由于人为制造虚假信息可能导致服务的不可信(例如对消息收发和消息内容予以事后否认)的服务流程应配置有可信第三方参与的抗抵赖措施。

4）防火患与水患

火患和水患能破坏信息设备和信息的可用性。面对此类风险，采取的安全措施如下。

- 物理保护：对于所有放置信息设备和存储介质的建筑物和房间都应采取防火、防水措施，并设立醒目的警示性标志和语言。
- 备份预案：为应对突发的系统不可抗拒的水灾和火灾，应制定并实施业务连续性方案，并对所有用于恢复系统业务的系统管理信息和业务数据进行备份。

5）防维护误操作

在定期维护工作中出现误操作可能导致系统运行混乱或系统不能按预期运行，面对此类风险，采取的安全措施如下。

- 按规程操作：按操作规程进行系统维护是避免维护出错的最有效的办法。需要特别说明的是，在维护中如需对某些设备或组件进行拆卸和重装，在动手拆卸前要对这些维护点的现场（软/硬件形态和系统状态）进行详细记录，以供恢复现场设备或组件时进行核对。
- 备份：如果发生维护操作错误，通过备份数据可以帮助恢复到维护前的状态。

6）防完整性破坏使可用性丧失

系统和组件的完整性被破坏可使信息系统丧失可用性。面对此类威胁和风险，采取的安全措施与保护数据完整的措施完全相同，需要时可参见“维护完整性的安全措施”的相关内容。

7）防信息错误路由

信息的错误路由指故意或意外地将信息引导到错误的传输方向或攻击者预期的接收地，从而引发系统服务出现混乱。面对此类风险，采取的安全措施如下。

- 网络管理：确保路由表不能被未授权修改，将修改路由表的权限授予范围控制到最小。
- 抗抵赖：对可能由于错误路由而引发信息混乱，导致系统服务出错的，在信息的源地和宿地加装抗抵赖功能，核实信息的真实来源。

8）防资源滥用

对资源的滥用会导致信息的不可用。面对此类风险，采用的安全措施如下。

- 纪律约束：每个员工都应意识到滥用资源可能引起的后果和自己应承担的责任。
- 操作方面：严格禁止对系统硬件设施进行未授权操作，在必要的地方安装视频监控系统，监视未经许可的活动；可对关键设备的操作任务进行分割，以使滥用职权的风险降至最低。
- 识别与鉴别：将适当的识别与鉴别措施与逻辑访问控制措施结合使用，增强对未经许可的操作的阻止能力。
- 逻辑访问控制：在逻辑访问控制机制中附加访问资源的约束条件，阻止越权滥用资源。
- 网络管理：通过适当的网络资源配置和操作权限分割限制或阻止未授权或越权滥用资源。

9）规避自然灾害

自然灾害可能对信息和设施造成灾难性的损害。面对此类风险，采取的相应措施如下。

- 增强建筑物的物理安全：针对自然灾害，应对建筑物进行符合国家技术标准的建设和保护（包括抗震、防洪水、防泥石流等主要技术指标）。
- 业务连续性方案：应制订业务连续性方案，并进行严格测试；对组织业务恢复所必需的数据进行备份，必要时可在异地备份一个最小集的软/硬件系统。

10）防软件故障

软件故障一般由软件缺陷在条件符合时引发，故障出现后可导致相关软件中数据和信息的不可用。面对此类风险，采用的相应措施如下。

- 使用正版软件：使用正版软件以获得技术支持，不使用正版软件的复制件。
- 报告软件故障：及时报告并修复软件故障，限制软件故障所造成的损失。

- 按规程操作：对使用的软件进行安全性能符合度测试，必要时对软件缺陷进行修复，以保证软件的正常运行；检测并消除软件中的后门程序；对软件的变更进行识别和控制，以防止软件更新时或软件要求的运行环境变更时，引发新的不可用问题。
- 备份：进行必要备份，以支持软件故障修复时能利用备份将系统配置数据和业务运行数据进行恢复。

5. 确保可确认性和真实性的安全措施

在不同领域的信息系统内对可确认性和真实性的要求是不一样的。相应地，应在不同领域的信息系统中实施不同的安全策略。因此，本节给出一般性指导建议。

1）可确认性

有些事件可能无法追查出引发风险的执行操作的具体人员。此类例子如共享账号导致缺乏对引起事件的具体操作的追溯能力，对用户身份的冒充，软件出现故障，对计算机、数据、设施及应用软件的未授权访问，这些都可能是原因。

有两种供选择的方法用来解决这一问题。一种是加强对负责具体操作的人员的身份的鉴别措施，可防止假冒身份进行操作的威胁；另一种是在信息系统用户组内对信息发出者和信息来源加装抗抵赖的措施，例如使用数字签名技术、知识分割技术和双向鉴别方法等，都能防止假冒身份、抵赖发送过信息和发送的虚假信息等威胁形式。

2）真实性

有些威胁方式会使用户、系统或处理进程不能确定某一个信息实体到底是真实的，还是经篡改过(或因传输故障引起失真)的，或是其真实来源，等等。例如信息在发送前被修改或在传输中丢失一些数据，使得接收者无法判断信息的真实来源，无法判断接收到的信息是发送前的原始信息还是失真的信息。

真实性和可确认性是一对伴生概念，真实性指操作实体(例如信息发送者)和始发地，以及实体操作的对象(例如发送者发送的信息内容)的客观存在；可确认性指对前述客观存在的真实性予以判断。没有真实性问题，可确认性就不存在；没有可确认性，真实性便无从谈起。

举例说明，有甲、乙两人(他们之间可能认识，也可能不认识)，甲说他从乙的朋友丙那里来，并给乙带来一封信，乙收到甲带的信并拆开阅读。如果一切都是真实的，谁也不否认自己做过的事，那么什么问题也没有。但这一事件过程可能出现两个情况。

情况一：乙看到信后，对甲是否从丙那里来，甲是否是他本人声称的身份，以及甲带给乙的信是否真是丙写的，途中有否改过等一件事或多件事或全部表示疑问。

情况二：甲在事后说未给乙带过信，或虽受托带过信但并未改过信的内容；乙在事后否认收到过甲带的信，或者否认信中的内容。在这些情况出现后便需要查实真相。这个例子中的所有疑问都是由于对真实性的怀疑以及无法确认真假造成的。

问题在于，有没有办法使甲、乙双方在过程中间判断真假，或使甲、乙双方无法在事后否认自己的行为(带过信或收到过信)和行为的内容(信的文字内容)呢？这就是真实性以及如何确认真实性的问题。

加强鉴别可防身份假冒，数字签名技术可确保信息的真实来源或检测信息篡改，增加抗抵赖功能可使当事人双方在事后不能抵赖自己的行为。

5.4.3.5　根据详细风险评估选择安全措施

根据详细风险评估结果选择安全措施时所遵循的原则与上一节相同，不过详细风险分析能从结构化方面帮助人们更为细粒度和更为准确地考虑信息系统及其资产的具体安全需求和对安全环境的要求。

在前面已介绍组织选择信息系统安全措施的几种策略，包括以下几种：

- 对信息系统的安全措施使用“基线”法进行选择，而不必通过正式的或详细的风险分析方法；
- 在对信息系统使用详细风险分析法后按照对抗风险的安全需求选择安全措施；
- 使用“组合方法”对信息系统风险进行分析，即先对信息系统中存在的高风险（点或区域）进行识别，然后对低风险的信息系统区域应用“基线”法选择一组“通用”的安全措施，并对高风险的信息系统区域使用详细风险分析法后，依照对抗风险的安全需求选择有针对性的安全措施。

下面进一步介绍对信息系统使用详细风险分析方法后，如何利用分析结果确定安全措施。

与安全措施选择有关的因素有 3 个方面，即脆弱性、脆弱性面监的威胁、威胁发生的影响或后果，这 3 方面在概念上具有递推关系。脆弱性是第一因素，威胁是第二因素，彼此存在因果关系；接下来的分析因素是影响，用于估计前两个因素形成的损失；当这 3 个因素确定后，根据事件发生概率和事件造成的损失即可判定风险及大小。

在决定对抗风险的策略（降低、消除、规避、转移或接受）后，需要考虑采用何种措施才能满足风险对抗策略的需要，也就是通常所说的安全需求。例如采用降低风险的策略来解决身份假冒的问题（安全需求），那么安全措施可以是加强身份鉴别等；如采用消除风险的策略来解决交易中的抵赖问题，那么安全措施可以是使用可信第三方参与并对交易信息进行签名的仲裁系统；如采用规避风险的策略来躲避风险，那么可以采用的措施是使用路由引导方法将威胁路径绕过脆弱点到达指定的可控制地址（例如蜜罐）；如采用转移风险的策略来减少所遭受的损失，那么可以采用的措施是通过购买保险的方式在事件后索赔；如决定采用接受风险的策略，那么采用的措施包括对残留风险的评估和对残留风险变化的监控。

安全措施对抗风险的形式列举如下。

- 降低脆弱性引发风险的概率和影响：安全措施可以消除脆弱性（例如安装补丁程序），降低脆弱程度（例如一个与外部网络相连的内部网络面对外部未授权访问显得十分脆弱，安装防火墙将使这种脆弱性大为降低，若采用物理方法与外网隔离则可完全消除此类脆弱性，等等）；
- 增加外部威胁攻击的难度：安全措施能降低威胁企图成功的可能性（如增加口令字的长度和口令构成复杂度并不断更换口令，可降低使用猜测方法获取口令的机会），即使面对某些恶意攻击，例如针对窃取敏感数据的威胁，适当的安全措施也可以阻止威胁企图的成功实施（例如增加密码算法的复杂度可以大大降低破译密码的成功率，甚至做到在密码生存期内无法破译）等；
- 降低影响：安全措施能减少或避免负面影响（例如，如果服务中断造成负面影响是由于通信线路和设备故障引起的，那么提高通信线路质量和对设备进行备份可以降低服务中断的时间间隔，如采用热备份基本上不影响服务）。

但即使是同一种安全措施，面对不同的风险或在不同的场合使用，其安全保护效果的差别可能非常大。在很多情况下，一个威胁可利用多个脆弱性实现对信息资产的攻击，反过来，一个脆弱性可能被多个威胁所利用。因此，如果一项降低脆弱性的安全措施是用来阻止某种威胁的发生，可能也会同时阻止另外的威胁，反过来，要阻止某一威胁，则可能需要采取多种安全措施降低或消除多个脆弱性。

要尽可能考虑这些关系所带来的相互影响或可能带来的额外安全利益。所有附带的安全利益也应该整理成文档，以对某项安全措施所能满足的安全要求有一个全面的认识。

一些软/硬件一体的安全设备综合了多种安全措施，能提供以下一种或多种类型的保护：预防、阻碍、减缓、检测、监控以及安全意识警示。至于如何配置和激活这些安全措施，使其达到最佳效果，这取决于信息系统的业务特点和具体环境以及每种安全措施的主要保护目的，同时还可能与管理配置的技术人员的业务素质和技能有关。在很多情况下，一项安全措施可提供多种保护及附加的安全利益。只要有可能，应尽量选择能提供多种安全措施的安全设备。

在涉及以上安全措施选择原则时，要考虑安全保护成本与安全效能之间的适度平衡。如果过于强调一种类型的安全措施的作用或对某些资产的安全保护强度，那么整体的安全性保障成本可能会提高。

在实施所建议的安全措施前，应将其与已运行的安全措施做一个比较评估。首先应考虑能否通过对现行安全措施的功能增强或升级来达到所要求的安全保护等级。因为与引入全新的安全措施相比，这样做的成本会低得多，而且安全措施的运行管理经验可以带来实际的安全利益。

在选择安全措施时，要对实施安全措施的成本与资产的价值、安全措施所带来的收益进行权衡。一方面，如果一种安全措施的购置和维护成本比被保护资产的价值高，就必须考虑采用这种安全措施的必要性和合理性；另一方面，如果安全措施的维护成本比安全措施本身的购置成本高得多，也应考虑实施后的维护问题。

一些技术上的约束条件，如对性能的要求、可管理性（对操作方面的支持要求）和兼容性问题等，可能会限制使用某些安全措施。在这种情况下，系统管理者应与安全管理者进行沟通协调以确定出最佳的解决方案。一般的安全措施都可能降低系统运行的某方面性能，但这可以在安全利益和性能之间求得平衡，性能降低的量以信息系统服务能力和工作人员可接受为最低要求。

隐私保护及法律约束可能要求一些特定的安全措施，因此要定义满足这些特定的保护和法律性要求的基本安全措施。

5.4.3.6 安全措施的实施

为了实施安全措施，要制订一个信息安全措施计划描述所有的必要步骤，负责这个计划的人（一般是信息系统安全官员）应保证遵照计划中的优先顺序和进度表安排。

为保证实施安全措施计划的连续性和一致性，安全措施文档应作为信息安全文档的一个重要组成部分，也是组织的安全文档的一部分组织编写。

信息安全文档是一系列文档的总和，包括安全措施计划、业务连续性计划、风险分析文档以及安全策略和各种规程等。它应该完整并能满足领导、用户、系统管理员、维护人员和参与配置和变更管理的人员的需要。它必须是通用的和足够详细的，以帮助消除由于安全

过失和疏忽所造成的影响，能提供保证安全操作正确和有效地执行所需的信息。很多文档，特别是关于脆弱性、威胁和风险的文档，可能是敏感的，应妥善保护起来防止未授权的泄露。因此，绝大多数组织都需要非常小心地处理这些文档，并且需要一种"可信的"的分发规程。分发规程也应以某种方式归档，包括描述安全措施的敏感信息如何被存储、访问和使用。此外，这个规程应确认谁负责决定被保护的信息如何存储以及谁可以访问和使用它。在分发规程的设计中，安全措施信息的可访问性应考虑到一些特别的因素，例如在灾难或其他不可预见的事件等情况下，由于时间的紧迫性，需要尽快找到和使用灾难恢复计划。最后，对安全措施文档进行严格的配置控制也是需要的，以保证不会做出未被授权的更改而造成无意地或无知地降低安全措施效能的后果。

一旦信息安全措施计划制订完成并获得批准后，安全措施一定要付诸实施。对安全措施的遵从性要进行复核和检测。进行安全遵从性复核、检测的目的是检查安全措施是否满足法律要求，是否被正确地实施，它们是否有效地运行和受到恰当的测试。安全测试可作为安全遵从性检查的一部分来进行。安全测试应按照安全测试计划进行，测试计划应描述测试方法、测试环境和进度表。如果渗透测试被风险评估证明有效，则可以使用渗透测试。另外，必须撰写详细的安全测试过程，并使用标准的测试报告。

对于信息系统和业务的任何重大变更都应该进行重新评审、重新测试，然后调整信息安全措施计划并重新获得批准。

在已经制定信息安全措施计划之后，实施安全措施是信息系统安全官员的责任。在实施过程中应考虑下列情况：

- 将安全措施的开销维持在批准的范围内；
- 按照信息安全措施计划的要求正确实施安全措施；
- 按照信息安全措施计划的要求操作和管理安全措施。

大多技术上的安全措施都需要操作及行政管理方面的补充和支持，绝不能单纯地依赖技术措施。

安全措施的实施同样需要进行安全意识的教育培训。需要特别参加安全教育培训的人员如下：

- 开发信息系统的负责人；
- 操作信息系统的负责人；
- 信息工程及系统安全官员；
- 参与安全管理（比如访问控制）的相关负责人。

当这些安全措施得到批准并实施后，就应该授权信息系统正式投入运营或提供服务。

5.4.3.7　安全意识教育培训

组织内的信息系统从管理者到员工的所有层次都应该贯彻执行安全意识教育培训活动的计划。没有基层员工的接受和参与，安全意识活动计划不可能获得成功。员工需要理解安全意识教育培训活动计划成功执行的重要性。

安全意识教育培训活动计划应该大力宣传组织的信息安全策略，并且确保所有人员完全理解与自己岗位有关的安全操作规程以及各种正确的行为规范。另外，安全意识教育培训活动计划应该包含系统安全规划中确定的信息安全目标、方针和策略。该活动计划至少应包括下列内容：

- 信息是如何分类的；
- 用户和组织应知的安全事件的含义；
- 组织的信息安全规划中所包含的目标、方针和策略；
- 待实施的信息安全措施计划以及待检测的安全措施；
- 信息保护的基本需求；
- 信息资产所有者或管理者的责任、作业描述和规程；
- 需要报告和调查各种破坏及攻击企图等事件和行为；
- 以未授权方式和越权方式行事的后果(包括纪律处置、法律惩处)；等等。

有效的安全意识教育培训活动计划有各种形式，例如宣传册、员工安全手册、海报、案例或演习视频、新闻报道、演练、专题讨论会、研究班、专题安全演讲等。重要的是，安全意识教育培训活动计划的实施应该考虑社会、文化、心理学和法律等方面的约束，努力做到权力和义务的平衡，强制与兴趣结合。

安全意识教育培训应该使组织中的每一个人受益，从正面影响人们的行为规范，引导并提高全体人员的责任感和成就感。提高每个员工的安全意识是各层次负责人的工作之一，因此他们应该制订相应的实施安全意识教育活动计划的策略。在大型组织中，信息安全意识教育培训活动的组织协调责任由组织的信息安全官员承担。

安全意识教育培训活动应该定期反复进行，既可以更新原有员工的安全知识，又可以使新员工了解这方面的情况，同时了解和熟悉新知识、新技术、新规程。此外，每一位新员工、每一位履行新岗位职责者以及新升迁者都应该受到安全意识的再教育，以了解自己新的责任和所需的新规程。将信息安全方面的知识融合到其他培训课程中是安全意识教育的有效方法。需要强调的是，安全意识教育培训活动计划是一个持续和长期的过程。

5.4.4 后续活动

后续活动在信息安全管理中至关重要，但却容易被忽略，已实施的安全措施只有通过实际业务运行中的检验才能证明其有效性。

后续活动的主要目的是保证安全措施如设计的那样发挥预期作用。经过一段时间的运行，任何安全服务或机制的性能都可能出现恶化。后续活动应适时发现这种恶化，并启动矫正行动，这是维持保护信息系统所需的安全水平的唯一方法。下面各小节描述的一些活动计划构成一个有效的后续活动的基础。

5.4.4.1 维护安全措施

对安全措施的维护包括技术的和行政管理的措施的维护，是一个组织的安全措施计划的基本组成部分。它是各层次安全管理的共同责任，包括以下内容：

- 协调和调度组织的安全资源以维护安全措施；
- 定期检查，保证安全措施的效能与期望值相符；
- 重新初始化密钥种子值或计数器值等；
- 发现新的需求时，更新或升级安全措施(例如升级到新版本)；
- 明确维护安全措施的责任；
- 维护信息系统软、硬件修改和升级后不得改变已有安全措施的效能；
- 推行新技术不应该导致新的脆弱性和威胁。

在执行上述这些维护活动后，已有的安全措施将会持续发挥作用，负面影响也会尽量避免。

5.4.4.2 安全遵从性

与安全审计和安全评审类似，安全遵从性是保证信息系统安全计划一致性和连续性的基础性活动。

为了保证合适的安全等级，极为关键的是使已实施的安全措施遵从和继续遵从法律、信息工程或系统安全策略和安全措施计划。在所有信息工程和系统中，遵从性在下列工程阶段中和施工点上是必需的：

- 设计和开发期间；
- 系统运行的维护期内；
- 更换系统组件和进行安全事件处置时；
- 等等。

安全遵从性检测必须由具有相应资质和技术能力的外部或内部人员（例如审计员）来完成。

对安全遵从性检测应精心计划和组织，并将其与其他安全管理计划的活动整合在一起。

现场检测特别有助于判断管理人员和使用者是否遵从具体的安全措施及规程。检测的结果应该明确指出安全措施是否实施、是否正确实施和被正确使用、部署的地方是否正确以及是否经过测试。如果发现某些安全措施没有遵从一致性的安全策略（例如一些安全措施与另一些安全措施存在功能冲突或安全措施的功能定义模糊等），应该制订更正计划并实施，更正的结果还应通过评审。

5.4.4.3 监控

监控包括人工和自动监控，是信息系统安全生命周期管理的一个关键部分。监控可以帮助人们提供清晰的管理建议：

- 和设置的安全目标和可接受的最低安全目标比较，安全措施是否必要和充分；
- 安全措施的效能是否令人满意，以及特定的安全保护措施是否发挥了预期作用。

所有关于资产、脆弱性、威胁和安全措施的改变都会对风险产生潜在的重要影响，及早对系统变更进行检测是监控活动的组成部分，可以更深入地理解潜在的风险。

很多安全措施都可产生一系列与安全相关的事件日志。对这些日志定期并尽可能使用统计技术进行分析，可以及早检测到风险变化的趋势和不利事件的发生。监控活动也应包括向相关信息安全官员报告检测结果，提出有量化指标的建议。

5.4.4.4 事件处理

发生安全事件后，必须针对每个安全事件发生的原因、过程和所造成的损失开展调研，从事件中取得经验和吸取教训。事件处理过程要即时对信息系统运行中出现的偶然或故意的安全事件进行检测和反应，因此应该编制事件处理报告和调查方案。信息安全事件调查的基本目标如下：

- 以一种有效的方式搞清安全事件来源、过程和危害，及时做出反应；
- 从事件中吸取经验教训以防止类似（包括与此关联）的事件再次发生。

对已制定的安全事件处理计划的活动进行预先定义，可使组织在计划的时间内做出相应

反应。安全事件处理计划必须以年-月-日-时-分的顺序记录所有事件和处理活动，这将有助于人们对安全事件的全面了解，帮助减少风险。在分析记录的安全事件信息时应注意下列问题：

- 何时发生了何事；
- 员工是否已按计划（包括所遵从的规程）做出反应，以及执行了哪些操作；
- 员工是否可及时获得所需的信息；
- 同类事件再发生时，员工应如何应对。

对这些问题的回答将有助于理解事件处理过程。

5.5 网络安全管理

5.5.1 网络安全管理概述

本部分描述网络安全管理的过程，包括识别和分析网络体系结构以及与通信连接特性、网络互连特性和应用有关的要素。为确定安全需求，必须识别这些要素可能面临的现实的和潜在的风险，可为安全措施的选择提供指南，为网络和通信方面的安全管理提供指导。

5.5.2 任务

为了识别与网络通信相关的安全需求和安全措施，需要完成以下任务：

- 识别与网络连接相关的网络体系结构和应用业务特性，以便为完成任务提供必要的背景知识；
- 识别网络连接类型；
- 评审网络互连特性以及互连的信任关系；
- 评审组织的应用业务运行特点与网络结构和连接的关系；
- 从风险评估分析结果中获得信息，确定与风险相关的要素，包括对通过网络连接交换信息的业务价值，以及通过这些网络连接以非授权方式可访问到的其他信息及其价值；
- 评估满足应用业务需要的网络连接的普遍性风险；
- 在上述活动的基础上导出满足应用业务正常运行的安全保护需求，设计出合适的安全保护体系；
- 建立文档，并审核安全体系结构的备选方案；
- 使用设计的安全体系，在安全策略指导下参照管理和技术标准将具体安全措施选择、实施和维护的任务在组织内部分配到具体部门或岗位。

图 5.13 解释了这一全过程，它识别和分析了与网络通信相关的确定网络安全需求必须考虑的因素。

在图 5.13 中，实线（箭头指向）代表过程的主要（连接）步骤，虚线（箭头指向）代表需要在此结合对安全风险分析结果的评审意见，共同识别出潜在的安全需求。

对于这一过程中的某些步骤，特别是“评审信息安全策略”和“评审网络结构和应用”这两个步骤，需要反复调整以保证一致性。例如：

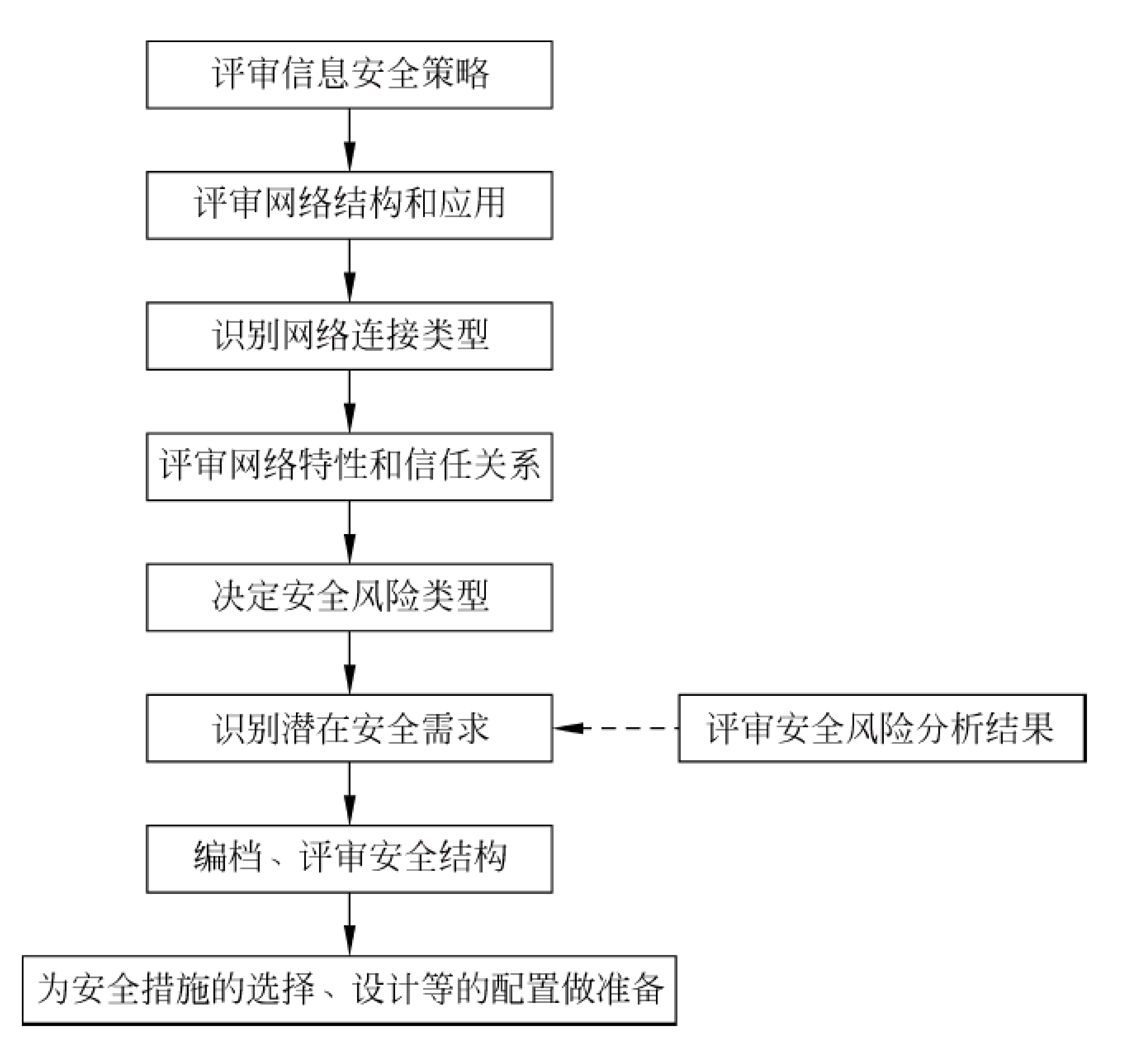


图 5.13　网络安全管理过程

- 在确定安全风险的类型后，也许需要再次评审组织的信息安全策略并进行必要调整，因为有些网络通信因素可能未被识别和考虑，但却需要反映在安全策略的某一层次结构中；
- 在识别可能选取的安全措施时，应该考虑组织的信息安全策略的某些刚性规定，例如安全策略可能规定某个(些)特殊的安全措施必须在组织内实施；
- 在审核安全体系结构的备选方案时，为保证兼容性，必须考虑网络的体系结构和应用。

5.5.3　过程识别和分析

5.5.3.1　组织的网络安全策略

组织的网络安全策略应该包括对必须保护的通信网络资源、面临的威胁进行分类，获得被保护网络资源机密性、完整性、可用性、可确认性和真实性保护的陈述。

例如，可用以下表述来说明一个策略：

- 重点保证通信网络带宽、网络设备的交换容量和性能，重点保护通信网络基础设施维持业务连续性的可用性；
- 防范来自外部对网络服务通道的阻塞；
- 防范来自内部人员对网络设备的未授权访问；
- 不允许内部计算机通过拨号电话线路绕过防火墙与外部网络连接；
- 网络内的所有用户必须经过安全网关才能与 Internet 连接，并接受审计；
- 选择安全网关必须同时保证遵从法律性规定和满足安全条件下的性能要求；等等。

(特别提醒，以上所列陈述并不具体针对某一信息系统的通信网络安全策略，而是一些策略条目的概念性陈述，不可在制定策略时直接套用。)

5.5.3.2 网络体系结构和应用

1. 概述

在网络体系结构和应用中需要考虑的问题如下：

- 网络的类型；
- 网络协议；
- 网络应用类型。

2. 网络的类型

依据网络覆盖的区域，网络可划分为以下类型：

- 局域网(LAN)：用于一个组织将本地的计算资源互连起来的相对独立的物理网络。
- 城域网(MAN)：用于在一个都市范围或一个综合业务地域内将多个组织的局域网互连起来的区域性物理网络。
- 广域网(WAN)：用于比城域网范围更大的区域将各种物理网络(包括局域网、城域网和远程通信终端)互连起来，直到采用 Internet 技术覆盖全球范围。广域网是一个广泛的概念，前述定义中的广域网可以指覆盖跨地区或国家的物理网络，也可以指在全球骨干物理网络上以国际互联网(Internet，因特网)通信协议组建的各种形式的虚拟专用网络的总称。

3. 网络协议

不同的网络协议具有不同的安全特性，因此需要分别予以考虑，例如：

- 共享介质的网络协议主要用于 LAN 中，有时也用在 MAN 中，这类协议使用 IEEE 802 委员会制定的系列技术标准，在互连的系统或用户之间提供机制来管制所使用的共享的网络介质。因为使用共享的网络介质，该网络上的所有信息对连在一起的那些计算机和计算机系统来说都是物理上可访问的。
- 路由选择协议用于在 MAN 和 WAN 中通过不同节点传送信息时定义传送路径。信息对在此路径上的所有系统来说都是物理上可访问的，并且路径是可以改变的。

不同的网络拓扑形式(例如总线型、环形和星形等)可以使用单一的网络协议，也可能同时使用多种协议(例如一个大型网络，骨干网络使用一种协议，而在内部局域网中使用另外的协议)，包括通过有线或无线技术实现的网络。这些网络拓扑中使用的网络协议从安全角度看是有区别的。

4. 网络应用类型

需要考虑网络应用类型与安全的关系，这些类型如下：

- 基于终端仿真的网络应用模式；
- 基于存储、转发和假脱机处理的网络应用模式；
- 客户/服务器(C/S)应用和浏览器/服务器(B/S)应用模式。

5. 其他考虑

当评审网络体系结构和网络应用类型对安全的影响时，还应该考虑存在于组织内部的连接以及“外部”与组织发生的网络连接。由于网络协议冲突或合同要求，组织已存在的连接也许会限制或阻止新的连接。“外部”进入组织或从组织向外部网络的连接将会引起额外的脆弱点，从而导致更高的风险，因此需要采用额外的安全措施。

5.5.3.3　网络连接的类型

一个组织可能需要利用不同的网络连接类型来满足多种业务需求。有些连接可以通过专用(物理)网络实现,有些可以通过公共网络实现(任何组织或个人都可以访问)。很显然,使用专用网络的连接与通过公共网络的连接,无论是自身的脆弱性还是面临的风险都大不一样。不同类型的网络连接也可以提供某些相同的网络服务,例如电子邮件、电子数据交换(EDI)等。当然,还可以使用因特网(Internet)和在其上组建的内联网(Intranet)、外联网(Extranet)以提供更广泛的个性化的企业或商业服务。每一种网络类型都可能面临相同的(共性)和不同的(个性)安全考虑,因为每一种类型的连接都有各自的脆弱性集合,其中有的脆弱性是共有的,有的是某种网络连接特有的,这就需要具体识别,从而确定相应的风险,据此选用不同的安全措施。

表 5.4 给出了网络连接的一种分类方式。

表 5.4　网络连接的类型

序　号	网络连接类型	描　　述
1	组织内,并在同一个控制区域内的物理连接	在一个控制区域内将同一组织内的不同部分之间互连起来,如单独控制的建筑物内的物理网络或局域网。组织外的用户不大可能未授权进入网络系统
2	同一组织内,处于不同地理位置的部分的相互连接	通过广域网或内联网将一个组织的区域分部(或区域分部与总部)之间互连起来。内部所有的用户都能通过该网络访问组织的信息系统,但并不是组织内的所有用户都有权力访问所有的应用和信息(即每个用户只能根据所授予的权限进行访问)。 组织可使用远程访问方式进行网络维护,这种连接类型的用户和连接需要更高的授权
3	组织的站点与远离组织的个人工作站点之间的连接(远程连接)	员工在家里或者其他远程站点通过网络与组织相连,使用移动数据终端访问组织的信息系统。用户在他自己的系统中被授权为系统用户
4	关系密切的不同组织间相互连接,即由于合同或其他法律绑定关系,或由于商业共同利益关系,例如银行业和保险业	在两个或更多的组织间通过城域网或外联网的互连。这种网络连接和本表第 2 种类型类似,不同的是这种方式中互连的站点属于两个或更多个组织,而且这种连接并不提供对每个参与组织的所有应用的访问权力,只在不同组织的相同业务部门或合作业务之间相互授权访问
5	一个组织与其他组织的连接	一个组织通过服务供应商的链接访问其他组织的远程数据库。在这种类型的网络连接中,组织内的所有用户需由被访问组织(其信息可提供访问)单独预授权。不过,这类连接可能访问到其组织内的某些应用程序的信息,而这些信息可以同时提供给内部和外部的用户。在这种情况下,应该知道访问信息的用户是来自外部并且获得授权的。反过来说,被访问的组织可使用这类连接对位于该组织外的设备进行远程维护,这就必须为使用这种访问连接方式的用户和连接授予更高的权限

续表

序　号	网络连接类型	描　　述
6	与公共网络连接	由组织的用户通过因特网的连接访问公共数据库、Web站点或使用电子邮件服务，连接目的是为了信息检索、访问公共资源和收/发邮件等，这类连接并不需要得到组织的特别的预授权。在这种类型的连接中，无论是获得授权还是出于个人目的，组织对此类行为很少或不予控制。不过，可能存在来自外部通过因特网对组织的信息设备进行访问的风险。而在这种连接类型中，组织对来自外部个人的访问一般不会单独特别地予以预授权

5.5.3.4　网络特性和安全可信度

1. 网络特性

网络特性包括网络类型及其安全属性，网络类型不同，其相应的安全属性可能存在差别。

一些专用于承载一般数据或应用程序的基础性网络的特性及其安全属性情况如下：

- 公共网络：任何人都可不经特别授权（收费服务许可除外）访问或利用的网络，这种网络几乎没有安全保证。
- 专有（用）网络：一个由组织自己组建或租用专线组成的网络，专为组织的特定业务提供网络支持，一般不对外连接，但可以通过特别通道与外网连接，而这类通道一般不授权组织内部个人使用，因此认为它比公网更安全。
- 交换网络：为不同局域网之间和使用异构网络协议的网络之间提供互连互通的网络基础设施，接入这类网络一般需要特别许可，并需安装相应的网络设备，这类网络的连接有临时性和永久性两种，其中临时性连接需要获得特别授权。

承载某类专业数据或信息并直接向社会提供服务的应用型网络的特性及其安全属性情况如下：

- 数据网络：主要指使用数据传输协议传输数据的服务型网络，这类应用网络的相互连接只授权给连接两端，没有获得授权或不理解传输协议者很难接入，但存在数据被窃听的风险。
- 语音网络：主要指使用专门协议传送语音和数据的服务型网络，安全特性同数据网络。
- 视频网络：主要指使用视频传输协议同步传送语音和图像的服务型网络，安全特性同数据网络。

2. 网络的可信度

确定了使用网络的类型，也就决定了网络的固有安全属性，进一步对网络运行环境和网络使用主体进行了解后，即可对各类基础性和业务性网络的可信度做初步估计。不过这里列出的可信度是从公共角度比较而言的，一般都不能作为组织内部定义的可信度加以引用，因为组织内部对网络的安全可信度要求一般还要高一些。

表5.5所示的阵列关系示意了各类团体网络与其可信度的关系。

表 5.5　团体网络的可信度描述

可信度	描　　述
低	未知的用户团体的网络，一般不可控
中	熟知的用户团体的网络，并且属于关系密切的业务团体(团体内有两个(含)组织)成员
高	熟知的用户团体的网络，并且只在一个关系密切的业务组织内

各类团体网络利用适用的网络(公网或专网)组网或连接的可信关系列于表 5.6 中(表中的数字 1～6 是表 5.4 的网络连接类型序号)。

表 5.6　信任关系识别

网络连接类型	可信度		
	低	中	高
公网	6	4	2
		5	3
专(私)网	4	4	1
	5	5	2
			3

表 5.6 为每一相关的连接确定一个可信度的参考值。

5.6　习题与思考题

1. 理解信息安全管理过程中一系列活动之间的逻辑关系(精读 5.1 的内容)。
2. 什么是残留风险和可接受风险？二者之间是什么关系？
3. 重点阅读 5.4.3.4 节的内容。
4. 为什么说信息系统资源(资产)的脆弱性与所面临的威胁具有因果关系？这种内在关系对于思考对抗威胁的方法有什么启示？举例说明。
5. 3 种风险分析方法分别适用于哪些类型的信息系统？
6. 在信息安全管理过程中，其核心思想是围绕控制风险展开活动，为什么要这样做？
7. 如果一个信息系统包括 3 个子系统，其中一个子系统为内部封闭运行的子系统，一个子系统为处理单一业务但与公共网络连接的子系统，一个子系统为处理综合业务信息并与多个外部信息系统连接的子系统，在风险评估中应如何选取适当的风险分析方法？

CHAPTER 6

第6章 信息安全管理的实施

信息安全需要采用技术和管理手段来实现。信息安全管理的任务包括：①信息系统风险评估(评估信息系统及资源的价值、评估信息资产的脆弱性、评估信息资产脆弱性面临的威胁、评估资产受到威胁后潜在的损失和对组织的影响、全面评估安全风险的分布及等级)；②根据风险导出安全需求；③根据安全需求选择并实施安全控制措施；④评估实施安全措施后的残留风险，并决定是否接受残留风险；⑤开展后续(跟踪)活动等。

为完成上述任务，信息安全的管理活动包括建立安全机构；制定组织的信息安全规划；制定完成各项信息安全任务的安全管理策略；对资产进行分类并落实责任人，实施控制；分配并落实各类人员的安全责任；保障物理和环境安全；维持业务过程的持续性；管理信息系统及环境的变动；管理信息系统安全设备的配置及变动；检测、监控和审计信息系统的安全状态；处置信息系统故障和安全事件；各类遵从性检查；制定和组织实施信息安全意识培训与业务持续性演练计划。

在这些信息安全管理活动中，将采取信息安全控制措施来维护信息安全。典型的控制措施有编制信息安全管理策略文档、信息安全责任划分及分配、信息安全意识教育与培训、信息安全事件处理、管理应急计划的实施等。

一个组织能否成功地实现信息安全，以下管理要素常常是至关重要的：准确制定确保组织业务目标实现的安全目标、方针和策略；安全管理策略与组织的文化背景和人文环境相适应，有利于员工自觉地接受管理，增强员工对信息安全的责任感和荣誉感；管理层明确地承诺并实施对信息安全在人力、财力和行政措施上的支持；准确地识别信息系统资源及其价值；正确的风险评估方法和准确的安全需求描述，恰当地选择安全措施；反复向所有的管理人员和一般员工灌输信息安全理念，提高安全意识；向所有的员工和签约合作方发布关于信息安全策略与标准的指南，解释本组织的信息安全策略与技术标准的正当性和严肃性；提供对组织内与信息安全有关的人员分类、分层次的信息安全培训和教育；建立综合的和平衡的评估体系，评估信息安全管理性能以及员工所反馈的改进建议。

以上是有关信息安全管理的基本要点，下面的内容将详细描述其中重要的概念和管理实践。

6.1　信息安全管理规划

信息安全管理规划是组织的信息安全总体规划的组成部分，是信息安全管理活动的规范性文档。组织应为信息系统的安全管理制定一套清晰的管理规范，并通过在组织内发布和维护信息安全规划，表明对信息安全的支持与承诺，达到为信息安全提供管理活动的指导和支持的目的。

6.1.1　管理规划文档

信息安全管理规划的文档应经管理层批准后以适当的方式发布或传达到所有员工。该文档应该陈述本组织管理信息安全的原则和方法。信息安全管理规划应该包括以下内容：

① 定义信息安全管理的目标、方针和策略，说明信息安全管理作为一种保障措施为实现信息系统安全所起的不可替代的作用；

② 陈述管理层从人力、物力和财力等方面支持实现信息安全管理策略的承诺；

③ 对组织有重大普遍性安全意义的安全管理策略中的规则和遵从性要求做必要说明，例如：

- 遵从法律和合同的要求；
- 安全意识教育培训的要求；
- 对计算机病毒和其他恶意软件的防范和检测；
- 业务持续性的管理要求；
- 违反安全策略必须承担的纪律或法律后果。

④ 明确信息安全管理的共同的和特定人员的责任，包括报告和处理安全事件；

⑤ 陈述与其他支持安全规划的文档（例如特定信息系统的特殊安全管理要求，或用户应该特别遵守的安全管理规则）的关系。

6.1.2　对规划的评审

信息安全管理规划应由专人负责维护，并按照既定的程序进行评审。

对信息安全规划的维护包括由于信息系统遵从的法律法规和组织安全规划变化、信息系统业务变化、运行环境变化、信息系统及其组件变化等引起的对信息安全管理规划的调整和更新，以及信息安全管理规划在管理实践中吸取系统管理员和用户意见进行的自我调整。

对信息安全规划的评审应确保不漏掉任何可能影响风险评估结果的原始依据及其变化，例如出现过重大的安全事件、发现新的脆弱性、组织的信息技术基础设施结构或使用的技术标准的变化等。同时，应对以下各项进行有计划的、定期的评审：

- 规划的有效性，可通过记录在案的安全事件的性质、数量和所造成的影响来论证和判断信息安全规划的有效性；
- 规划对业务运行效率的影响及需要的控制成本；
- 技术变化对规划有效性的正面或负面的作用。

评审应给出具体结果和意见，并提出是否需要改进或调整信息安全管理规划的建议。

6.2 组织对信息安全的管理

应建立安全管理框架来启动和控制在组织内实施的信息安全管理活动，以在组织内有效地管理信息安全。

6.2.1 信息安全管理的基本框架

应该按照5.4.1.2节的要求建立适当的、具有管理权威的信息安全管理委员会，履行批准信息安全策略，分配安全职责并协调组织内部信息安全管理实施的职责。如有必要，应在组织内建立信息安全咨询专家小组，并使其发挥作用；应建立与外部信息安全专家的联系，以跟踪行业发展趋势，跟踪信息安全技术标准和评估方法的发展，建立在处理安全事件时提供协作的联络渠道。另外，应鼓励多学科综合的信息安全管理方法，例如信息系统各层次管理者、用户、行政人员、应用软件设计人员、审计人员和保安人员以及行业(如保险和风险管理领域)专家之间的配合与协作。

1. 信息安全管理委员会的职责

信息安全管理委员会应该承担的主要职责如下：

- 向信息系统管理机构提供关于信息安全战略规划方面的建议；
- 审核信息安全策略，并提交信息系统管理机构批准；
- 监督信息安全管理活动；
- 评审组织的信息安全策略的有效性；
- 批准加强信息安全管理的重大变动行动；
- 对安全规划和信息安全活动中所需要的安全资源(人力、财力等)的配置提出建议。

应有一名信息安全管理员负责管理与安全有关的所有活动。

2. 信息安全管理的协作

对于较大型以上组织的信息系统，有必要成立由各相关管理部门的代表组成的跨部门的信息安全协调机构，以共同实施信息安全管理的控制措施。其主要职责如下：

- 协调组织内各信息安全管理部门之间的分工和责任；
- 协调信息安全管理方面的重大活动，如资产分类和风险评估；
- 协调和支持全组织范围的信息安全管理活动，如协调安全事故调查和安全意识培训计划等；
- 确保信息安全管理活动贯穿信息系统安全生命周期的全过程；
- 综合审核新系统或业务中的信息安全控制措施方面的充分性，并协调安全措施的实施；
- 加强全组织对信息安全管理活动的协调合作。

3. 信息安全责任分配

信息安全管理策略应该明确定义保护各种资产和实施具体的安全措施过程的职责。

应该用信息安全管理策略来指导组织内部信息安全管理任务和责任的分配，必要时针对具体的地点、系统和服务对信息安全管理策略做更详细的陈述，清晰地定义出各项有形资

产和信息资产以及业务流程的管理和使用方承担的责任。

在大多数组织中，应任命一名信息安全官员来具体负责组织与协调信息安全管理工作的开展和实施。但分配资源和具体实施安全控制措施的责任一般由各部门管理者承担，通常的做法是为每项信息资产指定专人来负责日常的安全管理工作。

信息资产的负责人可以把安全职责委托给相关部门的管理员或服务供应商。但信息资产负责人对资产的安全负有最终的责任，并有权根据规程或合同认定安全责任人是否恰当地履行了职责。

对各个层次管理者所负责的安全领域的责任进行描述时，应特别注意以下事项：

- 标识与系统安全管理有关的各种资产，定义对这些资产的安全管理规程；
- 各项资产或安全管理过程的管理者的责任应经过核准，并以文件的形式分发给责任人；
- 安全管理责任的授权规程应清晰地定义并记录在案。

4. 信息处理设施管理的授权

在对新的信息处理设施授权管理时，应考虑以下措施：

- 新的信息处理设施应有适当的管理制度，对用户的使用目的和使用权限进行授权，同时应得到负责维护本地信息系统安全官员的批准，以确保符合所有相关的安全策略和要求；
- 如有必要，应检查硬件和软件设施，以确保系统部件之间相互兼容；
- 使用个人信息处理设施处理业务信息和部署必要的控制措施时都应获得授权；
- 在工作场所使用个人信息处理设施可能导致新的脆弱性，因此应经过评估和授权。

上述控制措施在联网的环境中尤为重要。

5. 信息安全专家意见

许多组织都可能需要征求信息安全专家的意见，专家可由组织内富有经验的信息安全顾问和资深技术人员充当，也可外聘。组织可指定专人来协调专家意见和组织中对信息安全的认识，以达成共识，做出正确的安全管理决策。必要时，再聘请外部合适的专家组予以评审。

信息安全顾问为信息安全的所有方面提供咨询和建议。他们对安全威胁评估的质量和对安全控制措施的建议水平决定了组织的信息安全措施的有效性。为使安全建议最大限度地发挥作用，他们应有权收集和询问组织的各个管理层的具体意见。

若怀疑信息系统出现安全事件或资产遭受破坏，应尽早地咨询信息安全顾问或相应的外部专家，以获得专业性指导，并对受到威胁的资源进行调查或采取补救措施。尽管一般的内部安全调查是在管理层的控制下进行的，但仍应听取安全顾问更为专业的建议，以加深对问题的理解，帮助做出准确判断。

6. 组织间的合作

组织应和信息系统安全的国家执法机关、主管机构、信息服务提供机构以及通信网络营运部门保持适当的联系，并积极参与信息安全业界组织的论坛和技术交流活动。

在与机构外组织交换信息安全管理信息时必须遵守规定，不得将组织的信息安全管理信息泄漏给非授权的组织或人员。

7. 信息安全的独立审计

组织对信息系统安全的审计工作应该独立进行，以确保组织的安全措施能够客观地反映安全策略的执行，并且是有效和充分的。审计的目的是对安全措施的合法性(法律性依据)、合理性(技术标准)、有效性和充分性(测评)给出符合性结论。

审计工作应由组织内部的审计职能部门、独立经理人或精通此种审计工作的第三方机构来实施，审计人员必须具有相应的从业资质和能力。

6.2.2 第三方访问的安全管理

对第三方访问组织内部的信息和信息技术设施必须进行控制，以保证第三方访问不会对组织的信息和信息技术设施带来安全威胁。

若业务上需要第三方的参与，应对第三方参与的必要性和风险进行评估，并采取相应的安全控制措施，确保第三方的参与活动是可控的。所采取的安全控制措施应知会第三方，并在合作合同中明确指出。

第三方的访问活动中可能涉及与第三方有关的其他实体(组织、计算机、业务等)，在授予第三方访问权时应该考虑到第三方可能将访问权转让给关联实体，可增加额外措施(包括附加访问控制条件)，防范可能由第三方关联实体带来的安全风险。也可在与第三方的合作合同中说明不得擅自将授予第三方的访问权转让和泄露给关联实体。

在决定将信息处理业务进行外包时，对外包业务承包方访问信息系统的安全管理必须作为签订外包服务合同的必要附加条款。

1. 识别第三方访问的风险

第三方可能访问的资源类型如下：

- (物理访问)办公室、计算机房、文件柜等；
- (逻辑访问)组织的数据库、信息系统的信息和信息处理设备等。

当业务上需要第三方参与时，要对第三参与的风险进行评估，若现有安全控制措施不足以防范第三方参与的风险，必须增加额外安全措施。

风险评估必须考虑第三方的访问类型、被访问资源的价值、对第三方访问的现有控制措施以及这些访问可能给组织的信息系统安全带来的后果；按照合同规定必须在信息系统现场滞留一段时间的第三方人员存在的安全隐患也要考虑。

2. 与第三方签约时的安全管理

当涉及第三方访问本组织信息及信息技术设施时应签订正式的管理合同。该合同应包括所涉及的安全要求的细则，以使第三方理解本组织的安全策略和安全标准，遵守安全操作规范。合同条款的陈述应确保本组织和第三方之间对信息安全的理解一致。

组织在决定与第三方合作时，应考察其具备的资质和服务能力，以及社会信誉度。

在合同中应该考虑以下条款：

- 信息安全的总体目标；
- 资产保护方面，包括：
  - 参与保护组织资产(包括信息和软/硬件在内)的具体内容；
  - 对资产受到危害(如数据的丢失和被篡改等)时认定责任的方法；
  - 在合同截止期或合同执行期间的某一个双方同意的时间段内，确保第三方归还或

销毁因工作需要借用组织的信息系统的控制措施；
- 资产完整性和可用性的验收方法；
- 对合作期间复制和泄露信息的限制措施。
- 对每一可用服务的描述；
- 第三方服务等级的要求和服务不可接受的判断指标；
- 第三方人员调换的规定；
- 协约方各自的责任；
- 法律方面(如数据保护法规)的责任，当协约方涉及不同国家的组织时，还应考虑不同国家法律条款的区别；
- 知识产权和版权转让以及合作成果保护的规定；
- 对第三方访问控制的约定，包括：
  - 服从组织的访问控制方法或遵守双方约定的访问控制方法，对第三方使用独特的标识符(如用户 ID、口令等)的控制规定；
  - 第三方访问许可和权限的授予过程；
  - 记录第三方获准使用信息系统资源的用户以及他们行使权限的信息。
- 对可验证的性能进行定义；
- 监视和撤销第三方行为权力的约定；
- 组织审计或委任第三方审计合同执行情况的约定；
- 建立解决合作过程中出现问题的流程，必要时还要考虑应急安排；
- 软件、硬件安装和维护的责任；
- 双方认同的清晰的报告结构和报告形式；
- 合同变更的管理流程；
- 对第三方用户和管理者的操作和安全意识的培训；
- 防范第三方访问引入恶意软件的控制措施；
- 报告、通知和调查安全事件和安全损失的安排；
- 对第三方和连带承包商安全责任的界定；等等。

6.2.3　委外管理

当决定将组织的信息系统的运行、维护或信息处理的责任委托给其他组织时，要确保委外服务过程中组织的信息的安全性。

应该在签订的委外服务合同中表明通信网络、数据库、业务流程和桌面所面临的环境方面的风险，以及相应的安全控制措施和管理规程。

委外合同中的安全要求要征得双方同意。

委外管理者的合同条款可在 6.2.2 节的内容中进行选择。

6.3　资产的分类与控制

6.3.1　资产清单

应该编制并保持与每一个信息系统相关的资产的清单，清晰地识别每项资产及其拥有

者、管理者和使用者，以及资产的当前位置。编制资产清单是风险评估的基础和依据。

与信息系统相关的资产如下：

- 信息资产：数据文档、系统文件、用户手册、培训资料、操作和支持程序、持续性计划、备用系统安排以及供访问的信息等；
- 软件资产：应用软件、通信软件、系统软件、开发工具和实用程序等；
- 有形（硬件和物理）资产：计算机及外围设备（PC 机、服务器、工作站、监视器、存储设备、调制解调器、显示器、输入/输出设备等），通信设备（路由器、数字交换机、传真机、应答机等），交换介质（磁盘、光盘、便携式存储设备等），传输线缆（光缆、同轴电缆、双绞线缆等），机房设施（电源、空调设备等），家具和建筑物等；
- 无形资产：计算和通信服务、服务能力、版权、品牌和形象等。

应该对所有重要的信息资产予以识别并指定负责人，落实对其保持适当控制措施的责任。实施控制措施的职责可以委托，但指定的资产责任人应对资产损失负最终的责任。

6.3.2 信息的分类

信息有不同程度的敏感性和重要性，一些信息可能需要额外级别的保护和特殊处理。应该对信息进行分类，以指明保护要求、优先级顺序和保护等级，确保信息资产受到适当级别的保护。

根据信息的安全属性遭损坏后的影响程度确定适当的信息保护等级，同时考虑对特殊信息处理设施的安全保护的等级要求。

1. 分类准则

信息分类和相应的信息处理设备的保护控制措施应该考虑信息在共享过程中的限制要求以及对相关业务的影响，如对信息未经授权的访问或损坏可能造成的直接后果或对业务的间接影响。

分类原则应该具有预见性，并考虑到信息在分类后可以根据环境或系统变化按照安全保护策略的某些规定进行变更。

对信息进行分类的类别数量不必强调所有的信息系统都一样，而应根据信息系统的实际情况确定，以维护信息保护的最佳效费比例原则。

2. 信息的标识和处理

根据所采用的分类方案为信息的标记和处理制定合适的操作规程。这些规程的适用范围必须覆盖以物理或电子形式存在的信息资产。对于每一个信息类别，均应定义处理的操作规程，包含对下列种类的信息处理规程：

- 复制信息；
- 存储信息；
- 以普通邮件、传真和电子邮件传递信息；
- 以口头方式传送信息，包括使用移动电话、语音邮件、答录机等传送的信息；
- 应予销毁的信息。

敏感或重要的信息应该以适当的方式进行类别标识，该标识应该反映分类准则，标记的对象还包括打印报告、屏幕显示、记录信息的介质（磁带、磁盘、光碟、盒式磁带），标识的内容包括信息的敏感度级别、信息宿主、信息记录方式和共享范围等，必要时还应对信息的读/写

属性予以标识。

6.4　人员安全管理

6.4.1　雇用和解雇

在新员工聘用上岗前，应向其明确安全责任并包含在聘用合同条款中；在员工的雇用期间进行在岗培训和监督，以降低人为的操作失误，防范盗窃、诈骗或滥用设备或信息的风险。

对新员工在职业素质和技术能力进行充分的筛选，尤其是从事敏感信息处理工作的员工；所有员工以及第三方（例如产品供应商、信息安全咨询服务商和工程队伍等）的人员都应该签署保密协议。

1. 岗位责任中的安全

对安全管理角色及其承担的责任以文件形式规定。这些角色的责任应该既包括实现或保持安全策略的一般责任，又包括保护特定资产或执行特定安全过程或活动的具体责任。

2. 人员选拔及方针

对长期雇用员工的安全审查应该在招聘时进行，包括以下事项：

- 审查能力、职业操守的推荐材料；
- 考核应聘者所学专业课程情况；
- 确认所声称的学术或专业资格；
- 核对个人身份（身份证、护照或类似证件）的真实性和有效性。

当该员工的岗位具有访问信息或信息处理设备的机会，特别是涉及敏感信息，例如财务信息或高度机密的信息时，组织应该附加信用度审查。对于拟担任有相当权力职位的人员，这种审查应该定期重复进行。

对于承包方和临时员工应该执行类似的筛选程序。若这些人员是由代理机构推荐的，则在与代理机构签订的合同中明确规定该代理机构的推荐责任。如果由于某种原因不能完成筛选工作或者对筛选结果不满意，必须循环进行筛选或中止推荐程序。

管理层应该对有权访问敏感系统的新员工和缺乏经验的在岗员工进行必要的技术和管理知识培训，并加强安全监督工作，保证对每一名员工所从事的与安全有关的工作都受到定期的、来自更高层员工的监督和指导。

管理者应该意识到员工的个人环境和行为习惯可以影响他们的工作方式。例如个人收入问题、行为或生活方式的改变、重复的缺勤以及精神抑郁或情感挫伤等可能滋生员工欺诈、偷窃、操作失误或其他安全隐患，应该注意并据此充分考虑这类因素对信息安全保护的影响。

3. 保密协议

保密协议用于明确协议双方在员工受雇和解雇后一段时间内保守相关信息的秘密，以及为保守秘密必须遵守的行为规范和应承担的义务。通常签署此类协议作为员工受雇的必要条件。

临时员工和第三方人员在被授予信息或信息处理设备访问权前应签署保密协议。

在雇用条款或合作合同条款发生变化时，特别是员工要离开组织或合同到期时，应该对保密协议的执行情况进行评审，并规定脱密期限及期限内的保密责任。

4. 雇用期限和解雇条件

雇用期限和解雇条件阐明员工在雇用期内的安全责任以及解雇的后续安全约束。在雇用期结束后，这些安全责任一般应该延续一段时间，包括员工无视安全要求和保密协议时必须承担的后果。

员工承担的与安全有关的法律责任和应享受的权力（如涉及版权或专利权共享权力，对雇主数据分类和管理的责任等）均应包括在雇用条款和解雇条件中，必要时在雇用期限中还应该说明这些责任可延伸到组织范围以外和正常工作时间以外（例如在家里或出差在外地处理组织的信息业务）。

6.4.2　员工的在岗培训

应对在岗员工进行安全管理规程和正确使用信息处理设备的培训，以尽量降低可能的安全风险，确保员工意识到对信息安全的威胁或危害的后果，并具有在日常工作过程中支持安全策略的能力。

组织中的所有员工以及相关的第三方人员应该接受适当的信息安全教育和培训，以及适应组织的安全策略和管理规程变化的培训。培训内容包括安全要求、法律责任和业务控制措施，以及被授权访问信息或服务之前正确执行操作规范，如登录方法、软件包使用的培训。

1. 培训模型

培训模型见图 6.1。

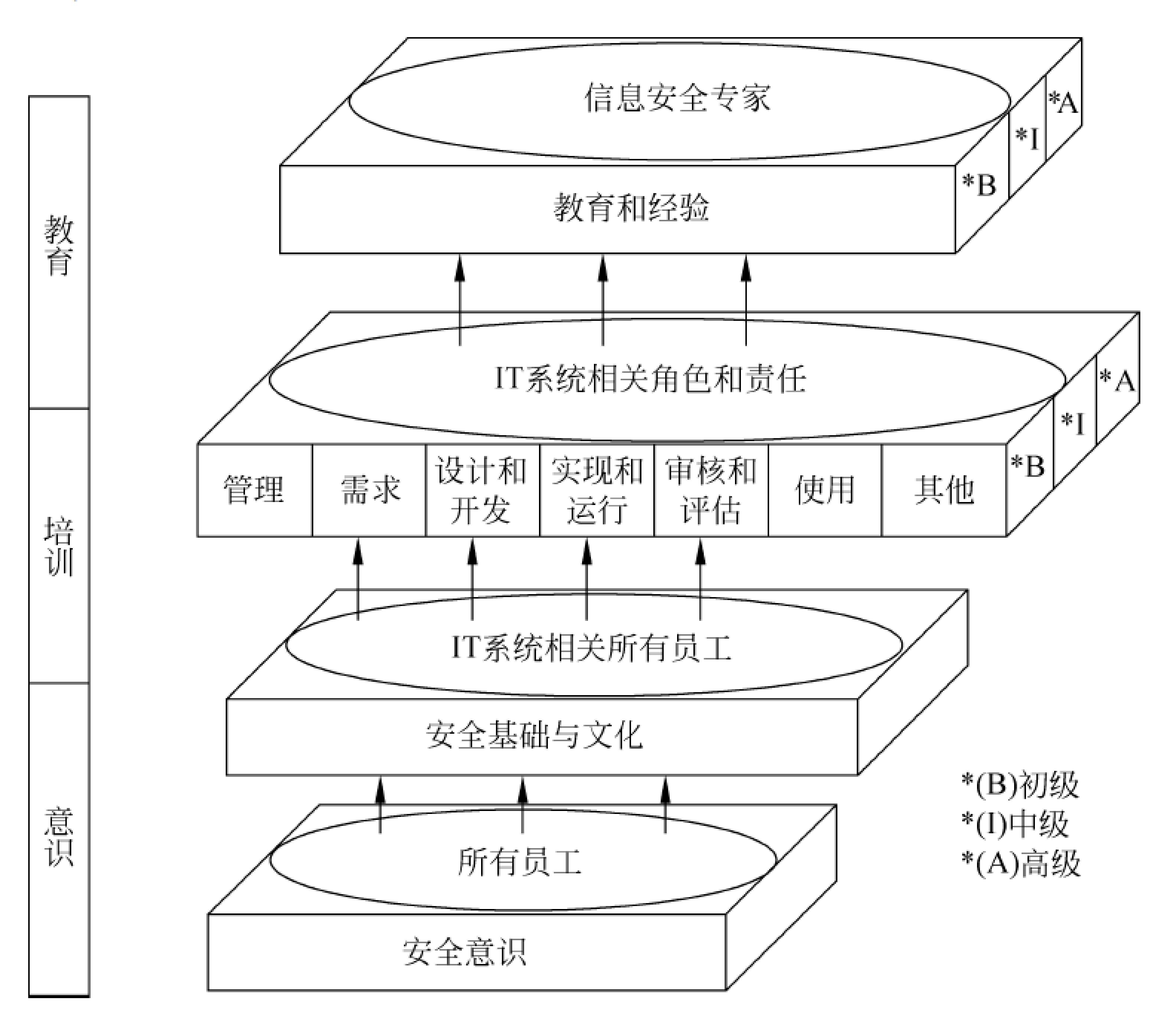


图 6.1　培训模型

2. 安全意识教育和培训

信息安全意识教育与培训过程是员工培训的重要组成部分，它将改变员工个人对信息系统安全的认识和态度，使他们认识到安全的重要性和安全失败所导致的不良后果。安全意识教育与培训过程对所有员工和第三方人员都是必需的。

信息安全意识教育与培训必须考虑到人们的接受能力循序渐进、逐步强化。如果只考虑刺激方式，起初能够引起人们的注意，但重复使用，学习者就会有选择性地忽略某些刺激。因此，安全意识培训必须是不断发展的、具有创新性的和有吸引力的，以吸引学习者的注意力，将那些条款式的规范和操作行为变为潜意识或习惯性行为。

总之，安全意识教育培训的目的是使员工对网络信息系统的脆弱性和面临的威胁保持敏感性，认识到需要保护的信息及正确的处理方法。信息安全意识培训计划的基本价值是使人们通过教育培训适应组织安全文化，因为安全出问题对每个人都会造成潜在的不利影响。因此，信息安全与每个人的工作和发展息息相关。

安全技能培训的目的是使员工获得所需的安全技能，以及信息安全之外的功能性专业知识(例如管理、系统设计和开发、部署、审计等)。安全意识教育应将所有的安全技能和各种功能性专业的能力整合成为一个通用的知识体系，通过对多学科的概念、原理和问题(技术上的和社会性的)等的学习和渗透、融合，从中培养出具有远见的信息技术安全专家和专业人才。

3. 在职安全教育

所有在职在岗的各层次的员工应针对实际工作需要不断接受管理、技术和安全意识方面的培训教育。

6.4.3 对安全事件和故障的响应

影响安全的事件和故障应尽快通过适当的管理渠道报告给有关人员和机构，以便调查事件原因和危害，必要时启动紧急事件应急处理计划，尽量减少安全事件和故障造成的损失，并吸取教训。

应使所有员工和合作的第三方签约人知道可能影响组织资产安全的不同种类事件的各种报告程序的规定，要求他们以最快的速度把看到的或可疑的事件报告给指定的联络人。为妥当地处理事件，有必要在事件发生后尽快地收集证据、组织调查、分析结果。

1. 报告安全事件

建立正式的报告程序，在安全事件或其预兆出现时，尽快通过适当的管理渠道报告给有关人员；建立安全事件响应程序，阐明接到安全事件报告后应立即采取的行动；建立对安全事件报告的反馈程序，以确保对安全事件报告的响应。

2. 报告安全脆弱点

应该要求提供信息服务的员工记录并报告任何察觉到的或可疑的系统或服务流程的安全脆弱点或对它们的威胁的预测，同时可依规程把这些问题向管理层或直接向服务供应商反映。另外，应该告知员工，在任何情况下都不应该擅自对被察觉的和可疑的脆弱点进行验证性测试，因为测试脆弱点可能滥用系统资源，并可能对系统造成致命损害。

3. 报告软件故障

建立报告软件故障的规程应该考虑以下步骤：

- 记录故障特征和显示在屏幕上的信息；
- 隔离有软件故障的计算机或信息处理设备，如果需要检测有软件故障的设备，应在重新启用前将其与组织的所有网络断开，存储的信息不能随意传送给其他计算机；
- 将事件立即报告给信息安全管理者。

除非获得授权，员工不得试图删除可疑的软件以修复故障，必须由经过适当培训并有经验的员工在授权状态下执行修复或恢复工作。

4. 从事件中学习

应该通过统计分析工具对安全事件和故障的种类、数量和损失进行量化分析，从中识别出安全事件的特征并进行观察和监控。这类信息有助于识别事件是初次发生还是反复发生，是偶然发生还是有条件发生，为事件的预测预防提供参考参数。

5. 惩罚程序

对违反组织安全策略和规程的员工应该有正式的惩罚规程，这样的规程对有意无视或无意忽视安全策略的员工将起到威慑作用。当然，也应该保证对被怀疑严重或连续破坏安全的员工处罚的准确性和公正性。

6.5 物理和环境安全管理

6.5.1 安全区域

关键或敏感的业务信息处理设备应该放置在安全区域，这一区域有规定的安全边界、适当的安全屏蔽措施和入口控制措施。存放在安全区域的这些设备应该受到符合国家标准的物理保护，防止未授权的接触、移动和破坏(安全区域和安全域是两个不同的概念。前者指有一定安全保证的区域。后者指信息系统中具有至少一个以上的共同安全属性，且遵守同一安全策略的信息系统组成元素的集合，是一个逻辑概念)。

所提供的保护措施应该能防范已知的风险。

在办公区内，建议采用清空办公桌面和清除屏幕显示的策略，以降低对文件、介质和信息处理设备的未经授权访问或破坏的风险。

1. 物理安全防护带

物理保护可以通过在业务场所和信息处理设备周围设置若干屏障加以实现，每个屏障形成一个安全防护带，安全防护带是构成屏障的某些东西，如墙、卡控门、有人值守的接待台等，每个防护带都能增强所提供的整体防护。每个屏障的设立位置和强度依据评估出的风险而定。组织应该使用安全防护带，以保护放置信息处理设备的区域。

应该考虑下述防护原则和控制措施：

- 明确规定安全防护带的边界和构成形式；
- 放置信息处理设备的建筑物或场所的防护带，在物理上应是相对固定和坚固的(如在防护带或安全区域不应有能轻易闯入的缺口)，场所的外墙应该是坚固的建筑物，所有的外门应该受到适当的保护，包括栅栏、警铃、卡锁等，防止未经授权进入；
- 应该设置有人值守的接待区或严格的隔离控制措施，对场所或建筑物实施出入的物理控制，对场所和建筑物的出入应该仅限于被授权的人员；

- 如有必要，物理屏障应从地板延伸到天花板，以防止未经授权地跨越或观察行为，隔离诸如火灾蔓延和环境污染；
- 安全防护带的所有防火门应具备报警功能。

2. 物理进入的控制措施

安全区应该通过适当的进入控制措施保护，以确保只有经授权的人员才能够进入，可考虑以下控制措施：

- 对安全区的访问者应该经批准并接受监视，同时记录进入和离开的日期和时间。他们应该仅被允许访问指定的、经授权的场所和目标，并发给他们关于安全区域要求和应急程序的说明。
- 对敏感信息和信息处理设备的访问应受到控制，并仅限于获得特别授权者。使用鉴别控制措施，例如安装身份标识的扫描卡，对所有访问进行身份鉴别和授权，并且应该对所有访问的审计日志进行安全保护。
- 应该要求所有员工穿戴某种明显的身份标志，并鼓励员工对没有陪伴的陌生人和没有穿戴明显身份标志的人进行劝离或盘问。
- 对安全区的访问权应该定期评审并更新。

3. 保护办公室、计算机房和设备的安全

在安全区内可能还有上锁的办公室或物理安全防护带内的若干房间。安全区的选择和设计应该考虑在火灾、水灾、爆炸、暴乱和其他形式的自然或人为灾害发生时的应对措施和疏散通道，遵从卫生规范和安全法规和标准，以及应对来自相邻场所的自然的威胁，例如来自其他区域的水泄漏或火蔓延。应该考虑以下控制措施：

- 关键设备的放置场所应该避免暴露；
- 建筑物不要过分显眼，并尽可能少地对外公布其用途，建筑物内、外不放置可表明存在信息处理活动的明显标志；
- 辅助功能和设备，例如影印机、传真机应该妥当地放置在安全区，以避免可能危害信息安全的盗用、误用或滥用；
- 房间在无人看管时门窗应该关闭上锁，必要的地方应该考虑对窗户，特别是落地窗户的外部保护或掩护；
- 应该在所有的外门和可以出入的窗户处按专业标准安装防盗系统并定期测试，无人区应该时刻保持警戒状态；
- 由组织管理的信息处理设备应该和第三方管理的信息处理设备物理隔离；
- 显示敏感信息处理设备位置的目录和内部电话本不应泄露给组织以外的人员；
- 危险或易燃物品应该安全地保存在与安全区有安全距离的地方，大宗消耗材料如文具等，除非有必要，只能在需要时才存放在安全区内；
- 备用设备和备份介质的放置应该与原系统设备和介质保持安全距离，以避免因灾害蔓延造成同时毁坏。

4. 在安全区内工作

对在安全区内工作的员工和第三方人员以及出现在安全区的第三方活动必须进行安全控制，应该考虑以下措施：

- 员工只有在必要时才能知道安全区的存在或其内的活动；

- 为了安全和防止产生恶意行为，在安全区内应该避免无人值守的活动；
- 空闲的安全区应该关门上锁并定期检查；
- 第三方服务支持人员只有在必要时才应该被允许有限制地访问安全区或敏感信息处理设备，这种访问应该经过授权并接受监督，在安全防护带内具有不同安全要求的区域之间可能需要隔离控制的额外屏障和防护带；
- 只有经授权才允许使用照相、录像、录音或其他记录设备。

5. 隔离交接区

安全区域与外部的交接区应予以控制。必要时应与信息处理设备隔离，以避免未经授权的访问，此类区域的安全要求应该由评估出的风险决定，可考虑以下控制措施：

- 从建筑物外对接货区的访问应限于经确认并予以授权的人；
- 应将接货区的结构设计成送货员能够卸货却无法访问建筑物的其他部分；
- 当接货区的内门打开时，外门应该有控制措施；
- 进入的物品在从接货区转移到使用地点之前，应该接受安全检查，以防止潜在的危险物品或物源流入；
- 如有必要，进入的物品应在交接区的入口处进行检查并登记。

6.5.2 保护设备安全

应该在物理上保护设备免受安全威胁和环境危害，这可以降低对设备未经授权访问的风险以及防止丢失或损坏，还应该考虑设备的放置和布局，必要的控制措施可以防止对信息处理设备和辅助设施的危害或未经授权的访问。

1. 设备放置和保护

应该合理地放置或保护设备，以降低环境威胁和危害造成的风险以及未经授权访问的机会。应该考虑以下控制措施：

- 放置设备的工作区应避免不必要的参观访问；
- 敏感数据的信息处理和存储设备应该与其他设备分开放置；
- 需要特殊保护的设备或物品应彼此隔离放置，以降低总体保护等级的需求；
- 应该采取措施尽量规避潜在威胁的风险，包括：
  - 偷窃；
  - 火灾、爆炸、烟雾、灰尘、震动；
  - 用水（或供水）故障；
  - 化学反应；
  - 电源干扰、电磁辐射，等等。
- 禁止在信息处理设备附近饮食和吸烟等行为；
- 对信息处理设备的运行环境应该进行监控；
- 考虑工业环境下设备的特殊保护方法（例如加键盘保护膜等）；
- 考虑发生在临近区域的灾害对设备的影响，例如邻近建筑物着火、天花板漏水、低于地平面的地面渗水或临街爆炸等。

2. 供电设施安全

应该保护供电设施以防电源中断和其他与供电有关的异常情况，根据设备制造商的要

求提供足够的电力，实现不间断供电的可选措施如下：

- 多条线路供电；
- 配备适当容量的不间断电源（UPS）作为紧急情况的应急供电；
- 配备备用发电机；
- 配备电源稳压装置。

在支持关键业务运行的设备上推荐使用不间断电源（UPS），以保证设备在异常断电时完成正常关机或保持持续运行，应急计划中应该包括 UPS 失效时所采取的应急措施。UPS 设备应该定期检查，以确保其有足够的电量维持指定的供电任务，并按照制造商的建议进行测试。

在可能出现长时间停电的运行环境中，应该考虑配备备用发电机。在安装之后，发电机应该按照制造商的说明定期测试，保证有足够的燃料供应，以确保发电机能支持到供电恢复。

另外，紧急电源开关应位于信息处理设备场所的紧急出口附近，以便在设备出现故障需要停电的紧急情况下迅速切断电源。为防电源发生故障时无法应对处理，机房和管理场所必须配备应急照明系统，并提供便携式照明装置。

为所有建筑物安装雷电防护系统，并在所有外部通信线路上安装雷电防护过滤器。

3. 线缆安全

应该保护传送数据或支持信息服务的通信电缆和电力电缆，防止窃听或损坏。通常考虑以下保护控制措施：

- 接入信息处理设备的电源和通信线缆应该铺设在地下管网或可覆盖的电缆沟内，或者采取其他坚实的保护措施避免暴露或破坏；
- 应该保护通信电缆以防止搭线窃听或破坏，例如通过使用电缆屏蔽管道和避免通过公共区域；
- 电力电缆应该与通信电缆隔离，并保持适当的安全距离，以防干扰；
- 对于敏感或关键的信息处理设备或系统的供电和通信线缆需要考虑附加的保护控制措施，包括：
  - 在电缆端子处外围加装坚固的保护箱柜并上锁；
  - 必要时使用可替换的路由选择或传输介质；
  - 传输线缆使用光纤电缆；
  - 自动或人工监控连接在电缆上的设备。

4. 设备维护

正确地维护设备，确保其完整性和持续的可用性，应该考虑以下控制措施：

- 设备应该按照供应商推荐的维护周期和规程定期保养和维护；
- 只有经授权的维护人员才能修理和保养设备；
- 对所有可疑的和确定的设备故障以及所有修复和纠正措施进行完整记录；
- 在将设备送到场所外维护时，应选择定点授权单位，并采取适当的安全控制措施（包括签订保密协议）。

5. 场所外设备的安全

经批准运行在组织场所外用于信息处理的设备，必须评估设备在组织场所外的风险，应

提供的保护强度应该等同于组织内相同用途的设备。这类信息处理设备包括托管在第三方机房的信息处理设备，以及用于家庭工作或从正常工作地点带出（例如出差在外）的所有形式的个人计算机、档案夹、移动电话、文件或其他的物品。应该考虑以下控制措施：

- 对于托管在第三方机房的信息处理设备应与第三方签订安全维护协议，要求第三方必须提供与组织内场所相同的安全维护强度，并履行保密职责；
- 从组织带出的设备和介质不得留在无可靠人员看管的公共场所，在旅行途中，移动计算机应该随身携带（人机不分离）并加以适当掩饰；
- 始终遵守生产商对设备保养的规定，例如不得暴露于强电磁场等；
- 对用于家庭工作的设备的控制应该通过风险评估，并采取合适的措施，例如文件柜上锁、清空桌面、清屏，设置不易猜测的进入计算机的口令等。

由于运行在组织场所外的信息处理设备所处的环境条件千差万别，其遭遇损坏、偷盗和窃听的安全风险差别很大，应该考虑与不同环境相适应的控制措施。

6. 设备的安全处置或再启用

不慎重处置或再启用设备可能泄漏信息。存储过敏感信息的存储设备在启用前，应该从物理上安全地删除，而不是使用一般的计算机的删除命令功能；存储过敏感信息的存储设备不再使用时，应采取物理销毁措施，如涉及国家秘密，则需交由保密部门指定的地点按指定的方法销毁。

设备内置的或外部配置的存储介质（如固定硬盘）设施，在进行销毁、送修和再启用前均应按规程进行严格的技术检查，以确保任何敏感数据和授权软件被彻底清除或物理重写；被损坏的存有敏感数据的存储设备需要经过风险评估后，决定这些设备是否应该销毁、修理或丢弃。

6.5.3 日常性控制措施

在日常工作中应注意保护信息和信息处理设备，以防信息被泄漏、修改和设备丢失或被偷窃。

1. 清空桌面和清屏

应考虑对放置在桌面的书面文件及便携式存储介质采取桌面清空策略，防止无人值守时遗留在桌面；对信息处理设备采取清屏策略，以降低在正常工作时间以外，信息被未经授权的访问、窃取和损坏的风险。这一控制策略的宽严度应考虑到信息安全保护等级、面临的风险程度和组织文化方面等因素的约束条件。

留在桌面上的信息存储介质还有可能被火灾、水灾、爆炸等灾害损坏或销毁。

日常性控制措施如下：

- 当书面文件和存储介质处于闲置状态时，特别是在工作时间外，应将其存放在上锁的柜子或类似的设备中；
- 载有敏感或关键业务信息的介质（包括纸质的或电子的）在不使用尤其是办公室无人看管时，应妥善存放在防火保险柜或密码文件柜中；
- 个人计算机和计算机终端等在无人看管时不应处于登录状态，应在空闲时段采用封锁键盘和锁屏/清屏等方式防范他人偷看或使用；
- 收发信件的场所和无人看管的传真机、电传机应该采取视频监控措施；

- 下班后应将复印机、传真机上锁(或者以其他方式防止未经授权的使用);
- 敏感或机密信息打印完后,应该立即从打印机存储区中将其清除。

2. 对资产搬移的控制

信息处理设备和存储介质等未经授权不得带离原场所,允许带离的应进行外出携带登记,并要求带离者履行安全保管和使用的责任。

6.6 常规性安全管理

6.6.1 操作程序和责任

制定所有信息处理设备的管理和操作规范,包括适当的操作指南和事件响应程序,确保对信息处理设备正确和安全地操作。

必要时,对重要处理设备的操作权限进行分割,并划分责任,以降低错误的操作引起的风险或故意滥用系统的风险。

1. 操作程序文档化

根据安全策略制定的操作规程应该文档化并加以维护。

文档化的操作规程应该明确规定每项事务流程的详细操作指导,包括:

- 信息的加工和处理流程;
- 服务的启动和关闭流程;
- 操作过程中出现错误或其他意外情况时的处理规程,包括对系统功能使用的限制;
- 发生意外的操作失误或技术困难时寻求支持的行动指南;
- 涉密信息输出的管理规范和失效作业数据输出的安全处理流程;
- 系统失效后重启系统或进行系统恢复的流程;
- 与信息处理和通信设备有关的系统日常管理活动的日志记录规范,如计算机启动和关机程序、备份规范、设备维护制度、对计算机房和信息处理设备进行管理的备忘记录规定。

2. 对变更的控制

对于信息处理设备和系统的操作规程的变更必须进行控制。在可行的情况下,应把业务变更和操作变更的控制流程整合起来,特别应考虑以下控制措施:

- 重大变更的识别和记录;
- 评估此类变更的潜在影响,必要时启动风险评估,确定残留风险是否可以接受;
- 重大变更的审批程序;
- 将变更的细节通知给所有相关人员的规程;
- 及时中止不成功的变更,并恢复到变更前的操作规程的审批流程。

3. 安全事件管理流程

建立安全事件管理责任制,制定管理规程,确保对安全事件快速、有序、有效的响应和处置,应考虑以下控制措施:

① 对下列类型的安全事件建立响应程序:

- 信息系统的服务能力丧失;

- 拒绝服务；
- 不完整或不准确的业务数据导致错误；
- 用户信息泄露。

② 除正常（为尽快地恢复系统或服务而设计）的应急计划以外，管理规程还应包括：

- 分析和识别事件原因；
- 如果有必要，设计和实施补救措施以防止事件的再次发生；
- 收集日志信息和类似证据；
- 与受到事件影响的人或恢复工作涉及的人进行沟通；
- 向有关管理人员汇报情况。

③ 如果有必要，收集并安全地保管事件线索和类似的证据，以用于：

- 分析事件发生的内部原因；
- 证明员工或第三方违反合同、违反法规要求或由此引起的民事或刑事诉讼（如由于滥用计算机或违反数据保护法）的证据；
- 与软件和服务供应商商谈赔偿问题。

④ 对受到安全事件影响的设施进行恢复以及对系统故障进行修复的行为均应受到正规和严格的控制，应确保：

- 仅允许经授权的员工访问运行中的系统和数据；
- 详细记录所采取的所有应急行动；
- 应急行动计划应报告给管理层，并按程序报批。

4. 职责分离

职责分离是降低意外或故意滥用系统的风险的一种有效方法。为减小未经授权的修改或滥用信息或服务的机会，适当分开管理或操作的职责或责任是非常必要的。

小规模信息系统可能发现这种控制方法难以实现，但这一原则还是应该以适当方式（包括简化措施）予以坚持。如难以对职责进行分离，可考虑采取相应的控制措施，如行为监视、审计跟踪和管理监督。在这种情况下，保持安全审计的独立性显得格外重要。

要特别提防在个人操作范围内出现的诈骗或监守自盗行为。

5. 开发、测试和操作分离

将开发、测试和操作设备的职责进行分离对实现系统正常运行非常重要，应该制定软件从开发转入运行状态的管理规则，并形成文档。

开发和测试行为不得由同一个（组）人来执行，也不得参与对同一台（组）设备的运行管理。类似地，开发和操作也不得由同一个（组）人来执行。

当开发和测试人员有权访问操作系统及相关信息时，有可能将未经授权和未经测试的程序代码或运行参数引入系统中，造成严重后果，轻则使信息系统的业务流程发生变更，重则使信息系统遭到不可预测的劫持。

如果开发和测试活动共享相同的计算环境，可能造成软件和信息的意外改变。因此，为降低意外改变或未经授权的访问操作软件和业务数据的风险，应将开发、测试和操作的设备进行分离。通常考虑以下控制措施：

- 用于开发的和操作的软件应该运行在不同的信息处理设备上，或者是置于不同的管理域或目录下；

- 开发、测试和运行环境必须分离；
- 编译程序、编辑程序和其他的系统软件在不需要时或未经许可不得擅自访问；
- 对操作系统和测试系统应使用不同的登录程序，操作菜单应显示适当的标识信息。

6. 外部设备管理

通过委外合同在组织场所外管理的信息处理设备可能存在潜在的安全隐患，如数据在承包商一方被泄密、修改、损失或遗失。应该提前识别这些风险，与合同方商定适当的控制措施，并将权利与义务写入合同。应该在合同中提出的特殊控制措施如下：

- 标识受委托保留在组织场所外的设备中的敏感或关键的应用软件；
- 受委托的第三方在维护信息设备需要访问业务应用软件时，必须获得设备委托人的授权；
- 要求受委托的第三方提供可持续业务计划；
- 详细陈述信息处理设备的安全保护标准和衡量符合性的约定；
- 监督所有相关安全活动的责任分配程序；
- 报告和处理安全事件的责任和流程。

6.6.2　系统规划和验收

对系统运行所需的容量和资源进行周密规划并留有余量，以达到将系统失效的风险降到最低的目的。

对未来容量需求要在计算后做出预测，以降低系统超载的风险。

在验收和投入运行前，对新的系统操作规范进行文档化并加以测试。

1. 容量规划

应计算所需的容量，并预测未来的容量需求，确保有足够的处理和存储能力可用。这些预测应考虑新业务和系统的需求，以及组织在信息处理方面当前的状态和未来的发展趋势。

管理者应使用这些信息来识别和避免可能对系统运行或服务流程造成影响的潜在瓶颈，并设计适当的补救措施。

2. 系统的验收

制定信息系统升级和新版本的验收标准，并在验收前对系统进行适当的测试。管理者应确保新系统的验收要求和标准被清晰地定义、文档化并经测试。验收应考虑以下指标：

- 系统性能和计算容量满足运行要求；
- 系统或数据的恢复和重启程序，以及应急计划；
- 测试日常的操作程序以达到规定的要求；
- 实施已通过审批的安全控制措施；
- 编写满足规范要求的操作说明书；
- 业务持续性计划的安排；
- 新信息系统的安装不会给现有信息系统带来负面影响的论证资料，特别是在处理量达高峰时；
- 已经考虑了新信息系统对组织的整体安全产生的影响；
- 对操作和使用新信息系统的各类人员进行培训的计划。

对于新系统中的技术或设备开发工作，应该在开发过程的所有阶段咨询系统管理员和

操作员，以确保所提出的系统设计方案的可操作性和运行效率，应该实施适当的测试来确认所有的验收指标已被满足。

6.6.3 脆弱性和补丁

补丁程序对减低或消除信息系统存在的脆弱性（点）是必不可少的。然而，人们最常犯的错误是没有或不及时为操作系统和应用软件打补丁。新的补丁程序可能不断发布，应通过正当渠道获得补丁程序。

脆弱性是信息系统资源（软/硬件形式的子系统、组器件）中的缺陷或弱点，它可能被敌对或恶意实体利用，从而在一台计算机上获得比被授权更多的访问权限。当然，并不是所有的脆弱性都有可用的补丁程序来修补；系统管理员必须意识到脆弱性的风险和相应的补丁程序对安全运行的作用。在无法通过补丁程序修补脆弱性时，可通过其他方法（如防火墙、路由控制表等）减轻脆弱性的影响。

为了帮助识别与安装日益增多的补丁程序，建议组织制订一个补丁分发使用策略，对使用补丁程序进行规范管理，可以建立一个识别和安装补丁和脆弱性机构（Patch and Vulnerability Group，PVG），在组织内识别和分发补丁。其职责包括：

- 建立一个组织的信息系统可能存在的脆弱性的清单；
- 识别新近发现的脆弱性和相应的安全补丁程序；
- 建立一个补丁库；
- 安装补丁程序前，对其进行功能性和安全性测试；
- 为本地管理员分发脆弱性信息和补丁程序；
- 通过网络安装补丁后，再进行主机脆弱性扫描；
- 培训系统管理员，学会利用脆弱性和补丁数据库；
- （适当时）部署补丁程序自动分发和安装模块。

即使组织建立了 PVG，系统管理员为他们管理的系统打补丁仍是必要的。每个系统管理员需要：

- 应用已被 PVG 识别的补丁；
- 在特定的目标系统中测试补丁；
- 测试与软件有关的没有被 PVG 识别的补丁和脆弱性。

6.6.4 防范恶意软件

需要有预防措施来检测和防止恶意软件的植入或渗透。

软件和信息处理设备易受渗入的恶意软件的攻击，包括计算机病毒、网络蠕虫和木马程序等。用户应该意识到恶意软件的危害，在需要的地方管理人员应该采取特殊的控制措施来检测和防止此类恶意软件的植入或渗入，特别是有必要采取预防措施来检测和防止个人计算机上的计算机病毒。

在实施防范恶意软件的监测和预防措施的同时，必须进行适当的用户安全意识培训。防范恶意软件必须强调安全意识，实施适当的系统访问控制和变更管理控制。一般考虑以下恶意软件防范和控制措施：

- 遵守软件许可协议并，禁止使用未经授权的软件或正版软件的复制品；

- 防范通过外部网络或从任何其他介质上下载文件和软件而引入恶意软件的风险，为此制定相应的安全措施；
- 安装和定期更新防病毒和木马程序的检测和杀灭软件，对计算机和存储介质进行病毒和木马扫描；
- 定期检查支持关键业务过程的系统的软件和数据内容，对出现的任何未经批准的文件或未经授权的修改应进行正式的调查；
- 对于存储介质上来源不明或来源未经授权的文件或者从不可靠的网络上下载的文件在使用之前进行病毒和木马检查；
- 对任何电子邮件的附件和从网站下载的内容在打开之前进行恶意软件检查。此类检查一般应在信息系统和外网之间的隔离区进行，如在电子邮件服务器、脱机的桌面计算机或进入组织的网络入口处；
- 定义防范病毒和木马的管理程序和责任，加强用户培训，及时报告发现的病毒和木马程序，并从病毒和木马程序的侵害中恢复；
- 制定受到病毒和木马攻击后的恢复计划，包括所有必需的数据和软件的备份以及对攻击的恢复安排；
- 建立验证与恶意软件相关的信息的规程，确保告警公告信息的准确性和可用性。管理者应确保资料来源是可靠的，如国家授权的预警中心、权威杂志、可信赖的网站或防毒软件供应商，以区分出恶作剧的虚假告警和真正的病毒来袭。管理人员应能识别恶作剧告警，并在收到恶作剧告警信息时进行适当处理。

这些控制措施对于支持大多数工作站、个人终端和网络服务器的防范工作是有效的。

6.6.5　内务处理

建立日常性备份制度对数据和系统或系统组件进行备份；制定快速恢复方案，并组织备份和快速恢复的演练；对所有操作事件和通信事件进行跟踪性的日志记录；在条件许可时，对信息处理设备和运行环境进行视频监控和人工巡逻，保持信息处理设备、通信环境的完整性和可用性。

1. 数据(信息)备份

业务数据(信息)、应用软件和系统运行所需的管理、控制信息都应该定期备份，应该提供足够的备份设备，以保证所有支持灾难或故障后迅速恢复必需的数据完整可用。不同系统的备份安排应该定期进行测试，以确保可以满足业务持续性计划的要求。在备份中应考虑以下控制措施：

- 为进行系统恢复需要备份一个最小集软/硬件系统，准确和完整的备份过程的记录以及文档化的恢复流程应该同时保存在 3 个不同的地点，以避免由于主场所发生灾害所带来的备份信息丢失或损失，对重要的业务数据、应用软件和系统性数据的备份地点应远离信息系统所属建筑物；
- 对备份信息的物理和环境的保护级别应和主场所保护的等级标准相一致，对主场所实施的控制措施适用于备份的场所；
- 对备份介质进行定期的测试，以确保紧急恢复时是可用的；
- 备份流程应定期进行检查和测试，确认其有效性，以确保恢复工作可以在规定的时

间内完成；
- 确定信息备份的保留期和备份更新周期，对需要永久保存的文档进行定期的更新性复制。

2. 系统操作日志

保留系统操作人员行为日志，日志应包括以下内容：
- 系统启动和关机时间；
- 系统错误和所采取的修正行为；
- 对数据文件和计算机输出的处理情况；
- 操作人员信息；
- 对操作人员的日志应按规范进行定期的、独立的检查。

3. 系统运行日志

对信息系统内的所有操作事件和通信事件进行跟踪式记录，在日志中应包括以下内容：
- 所有系统登录事件，尤其是多次尝试登录和登录失效事件；
- 所有通信事件，尤其是违规或外连通信事件。

6.6.6 网络管理

网络管理的目的是维持对网络中的信息和支持信息处理的设备、基础设施的机密性、完整性和可用性。对跨组织边界的网络的安全管理需要格外注意；对于通过公共网络的敏感信息要有额外的保护和控制措施。

由网络管理员实施网络控制，确保网络中数据的安全，并防止网络服务受到未授权的访问，特别需要考虑以下控制措施：
- 将网络配置操作和计算机业务操作的职责予以分离；
- 建立对远程设备(包括员工或用户操作区的设备)的管理责任和操作流程；
- 采取特殊的控制措施，以确保通过公共网络传输数据的机密性和完整性，并保护与外网连接的系统；
- 各种网络管理行为要紧密协作，以优化所提供的服务，并确保对信息处理基础设施的控制措施得以始终保持。

6.6.7 信息承载与流转过程的安全管理

对承载信息的存储介质应基于物理措施实行严格管理，应建立合适的操作规程来保护文档存储介质、计算机介质(磁带、软盘、盒式磁带、USB 盘、光盘等)的输入/输出数据和系统文件免受泄露、损坏、滥用或盗用，以及未授权的访问。同时，信息在流转过程中的每个环节也应有适当的安全保护措施，避免遭到未授权的泄露、修改和讹用。

1. 移动存储介质的管理

应有规程来管理可移动的计算机介质，如磁带、软盘、盒式磁带、USB 盘、光盘和打印/书写的文件，应考虑以下控制措施：
- 介质上的数据和信息如不再需要，应进行不可恢复的删除；
- 对从组织中换下来的任何存储介质都应妥善保存，并实行审核跟踪；
- 所有的存储介质应该按照制造商的使用指南保存在安全的环境中。

所有按规程处理的行为的授权情况都要记录在案。

2. 介质的处置

决定不再使用的存储介质应当按规程对其进行安全处理(包括使介质上的敏感信息不可恢复)。由于敏感信息可能通过对介质的草率处理而泄露,因此应当建立规范的介质安全处理流程将此类风险降至最低,应当考虑下面的控制措施:

① 对载有敏感信息的介质应进行安全、妥善的保存,如决定不再使用,则应采用安全的方式进行处置,如焚烧或粉碎,或在法律允许下清空数据后供本组织的公共数据存储使用;

② 需要安全处置的一些与介质(纸质的和电子的)有关的物品如下:

- 书面文件;
- 录音或其他形式的记录;
- 复写纸;
- 输出报告;
- 一次性打印色带;
- 磁带;
- 便携式磁盘或磁带;
- 光学存储介质;
- 规程列表;
- 测试的书面或电子数据;
- 系统文档;等等。

③ 把所有的介质收集起来集中进行安全处理比试图分离出敏感的介质进行单独处理可能更加容易;

④ 选择一个有足够控制措施和经验的机构对文件、设备和介质进行收购和处理;

⑤ 对敏感物品的处理要进行记录,以便日后复核。

将大量拟废弃介质积聚在一起等候集中处理时,应当特别注意"积聚效应",即大量的信息积聚在一起可能比少量信息更敏感。

3. 信息流转的安全控制

应当建立信息流转过程的安全管理措施,以便保护这些信息在流转的任何环节免于未授权的泄露或讹用;制定必要的管理规范,对含有信息的文件、计算机系统、网络、介质、移动计算设备、移动通信设备、文本、电子邮件、语音邮件、多媒体、邮政服务、传真机和其他敏感物品的使用进行控制,应当考虑下面的管理控制措施:

- 对所有介质进行标记;
- 对访问介质的行为进行限制,以识别未授权的人员;
- 正式记录数据的合法签收人;
- 对输出数据的安全保护措施与其敏感性的保护等级相符合;
- 把介质存放在符合相应的安全保护等级的环境中;
- 尽量减少数据的分发,并采取措施防范滥发数据;
- 对所有的数据副本进行清晰标记,以警示合法接收人员对其进行安全保护;
- 定期检查数据分发清单和合法收件人名单。

4. 系统文档的安全

系统文档一般都载有系统性的敏感信息,如对应用程序、业务流程、数据结构、授权过程的描述,应当考虑下面的控制措施,以保护系统文档免受未授权的访问:

- 系统文档应当按规定保存在具有物理保护措施的安全环境中;
- 对系统文档的访问必须按照规定经过相应的特别批准;
- 保留在公共网络上的或通过云端提供存储和应用的系统文档应当加密保护。

6.6.8 信息和软件的交换

在信息系统之间交换的信息和软件应该防止丢失、修改或滥用。在组织之间交换信息和软件,首先要对交换事宜本身的必要性和由此存在的安全隐患进行论证,然后对交换过程中的各个环节采取安全措施加以控制,并对数据传输过程进行全程保护。

6.6.8.1 信息和软件交换协议

在信息系统之间进行信息和软件的交换(通过电子的或人工的方式)必须订立协议,这些协议应该是规范的,必要时,包括由第三方保存软件的协议。关于安全交换的协议应当包括以下内容:

- 对数据发送、传输和接收3个过程进行控制的管理职责;
- 确定发件人和收件人的安全责任,将发送、传输和接收流程分发到发送人和接收人;
- 数据打包(包括数据封装和人工包装)和传输的最低安全保护要求;
- 约定信使的身份证明方法;
- 规定丢失数据的责任;
- 对敏感或关键的信息使用协商一致的标识系统,确保对标识的含义的一致性理解,使信息得到适当的保护;
- 确认信息和软件所属权及数据保护的责任,以及软件版权的合法性和类似考虑;
- 访问信息和软件的技术规程。

6.6.8.2 传输过程的安全

应当采用下列控制措施来保护信息在两地传输过程中的安全:

- 使用可靠的数据传输媒体(包括传输协议和线缆)或信使传输数据,并核查传输媒体和信使的可信性和可控性;
- 传送信息时应当使用安全的协议封装或坚固的物理包装,以保护信息和信息承载媒体免受传输过程中可能发生的逻辑的或物理的损坏;必要时,应当采用特殊的控制措施,以保护敏感信息免受未授权的泄露或修改;
- 对于物理性包装使用上锁的或加封条的包装箱;
- 传输方法包括隧道传输和加密传输、机要邮件渠道传输和人工专递;
- 使用防拆包的技术保护措施(例如完整性保护技术)和物理保护措施(例如密封箱外加密封条);
- 在利用网络传输的情况下,可将发送的信息分割成若干份,并通过不同的路线传递;
- 为防范信息内容在传输过程中被泄露,可使用数字签名和加密技术保护。

6.6.8.3　电子邮件交换的安全

电子邮件(E-Mail)是目前通过因特网(或在计算机网络之间)交换信息的最大众化的网络应用系统之一。

电子邮件服务器是最容易被攻击的目标之一。因为计算机和网络化技术支持的电子邮件都运行于因特网传输协议的基础上,为攻击者开发攻击模式提供了广泛的学习和演练环境,所以电子邮件服务器、客户机和支持它们的网络基础设施必须得到保护。对电子邮件的安全问题可列举如下:

- 电子邮件服务器应用程序中的缺陷可能被利用来攻击电子邮件系统;
- 拒绝服务攻击可以直接针对邮件服务器或支持它的网络基础设施,以拒绝或阻碍用户有效地使用邮件服务器;
- 电子邮件服务器上的敏感信息可能被来自邮件系统内部或外部人员未授权访问或修改;
- 在电子邮件服务器和客户机之间未加密传送的敏感信息可能被侦听或拦截;
- 电子邮件中的信息在发送者和接收者之间的某个转发点可能被截获或修改;
- 恶意实体可能在组织的计算机网络的其他地方通过对电子邮件服务器的成功攻击获得对资源的未授权访问,例如一旦电子邮件服务器被攻击者登录成功,攻击者就能够检索到用户的口令,这可能使攻击者获得其他主机登录邮件系统的权限;
- 恶意实体对一个电子邮件服务器主机成功攻击,进而利用电子邮件服务器作为跳板继续攻击其他组织的网络系统,这样就隐藏了入侵者的身份,并可能使电子邮件所属组织承担攻击的责任;
- 电子邮件服务器错误的配置可能被恶意实体利用,在电子邮件中插入广告或植入木马程序;
- 病毒和其他类型的恶意代码可能寄生于电子邮件,并利用电子邮件进行传播;
- 用户可能由于疏忽将电子邮件发送给不应接收该邮件的人;
- 用户可能通过 E-Mail 发送不合适的、私密的或敏感的信息,造成泄露秘密事件或引起法律诉讼。

下列措施可用来维护电子邮件服务器的安全。

1. 为电子邮件服务器制定安全保护策略

从电子邮件服务器的设计、技术开发到运维的各个阶段重视对从业人员的职业素质和技术素质的考察、培训和监管,因此需要考虑以下措施:

- 在选拔电子邮件服务器从业人员(如系统和邮件服务器管理员、网络管理员和系统维护人员)时,必须专门或在聘用合同条款中明确规定从业人员必须遵守职业道德,约定其为组织、用户保密的事项,并确认违反规定和约定事项必须承担的民事或刑事责任;
- 审核受聘人员必备的技能和能力资质;
- 强化定期的员工在岗培训。

2. 对操作和维护邮件服务器进行适当的安全管理或控制

适当的安全管理和控制措施对操作和维护邮件服务器非常重要,管理和控制措施如下:

- 制定严格规范的邮件服务器操作和维护规程;

- 对配置/变更电子邮件服务器运行参数的操作实行权限分割；
- 对邮件服务器的重大操作和维修事项的权限实行分割；
- 制定邮件服务器备份和灾难恢复计划。

3. 邮件服务器操作系统的配置和管理必须满足组织的安全需求

确保邮件服务器安全的基础性措施之一是要保证运行于邮件服务器底层的操作系统的安全。如果邮件服务器的操作系统关键性参数配置适当，可避免很多潜在的安全问题。一般地，邮件服务器供应商在交付时会设置一套硬件和软件初始参数作为服务器的默认配置，这些参数强调的是功能性能和易使用性，而很少从安全角度考虑。因为邮件供应商并不关注也不了解各个组织的具体安全需求。因此，组织必须在邮件服务器投入正常运营前，对其进行重新配置，以反映组织的安全需求并兼顾性能和易操作性。为此应注意以下措施：

- 对确认的邮件服务器操作系统的漏洞安装补丁程序；
- 删除或禁止不必要的服务、应用和脚本内容；
- 配置操作系统用户身份鉴别功能；
- 配置资源控制；
- 对操作系统进行安全测试和评估。

4. 实施加密技术以保护用户鉴别信息和邮件数据

大多数标准邮件协议对未加密用户的鉴别和发送邮件的明文数据是默认的。明文发送数据使攻击者很容易窃取用户的账号或拦截和改变未加密的邮件。大多数组织需要对用户的鉴别会话内容进行加密，即使它们不用来加密邮件数据本身。现在很多标准和专有的邮件协议支持对用户鉴别的会话信息进行加密。

对邮件数据进行加密的问题要大一些，主要在性能上。因为加密电子邮件对用户的计算机和组织的网络基础设施的运算和传输资源消耗很大。同时，还要考虑加入病毒扫描和邮件内容过滤，这就需要从管理上对安全和效率进行平衡。但对很多组织而言，邮件加密的好处远远超过为此所付出的运行性能代价。

5. 保护网络基础安全设施以保护邮件服务器

网络基础安全设施（如防火墙、路由器、入侵检测系统）对邮件服务器的安全保护起着重要的作用。在大多数配置中，网络基础安全设施将是因特网和邮件服务器之间的第一道防线。

6. 维护邮件服务器的安全

维护邮件服务器的安全是一个不间断的过程。因此，在日常维护的基础上对邮件服务器进行安全管理是邮件服务器安全的重要方面。维护邮件服务器的安全通常包括以下措施：

- 采集和分析邮件服务器的运行记录文件；
- 经常性地备份数据；
- 安装恶意代码（如病毒、蠕虫、特洛伊木马等）检查系统；
- 定期检测服务器脆弱性并及时打补丁，必要时对邮件服务软件进行更新或升级；
- 监控与审计。

7. 电子邮件内容过滤

电子邮件内容过滤是根据给定的关键词、特征词（汇）或短语对邮件内容进行判断以决

定是否接收或发送。它只是根据对文本文件进行字符一级匹配或相似度计算的结果来进行判断，而不在代码一级寻求过滤对象，因此不可能检测出恶意代码。通常，内容过滤和对病毒等恶意代码的扫描操作放在网络非军事区的同一个服务器中进行。

一般的邮件内容过滤的判断依据是关键词、特征词(汇)或短语出现的频度，以此基础进行统计分析很难对邮件内容的语义或语境所表达的意义作出判断，因此目前的邮件内容过滤结果都比较粗糙。尽管如此，对一些包含敏感信息或描述敏感事件的邮件进行审查时，这种方法在特定时段内或针对特定邮件收发群体还是有用的。如对邮件内容的过滤有特别要求，则应在上述过滤结果的基础上辅以人工判断。

6.6.8.4　其他形式信息交换中的完整性和真实性

对通过语音、传真和视频通信设备等进行信息交换的过程也要加以保护，保护的基本目的是防范信息在交换过程中被修改，以维持信息的完整性和真实性；有机密性要求的，需要防窃听；在需要防止未授权收发时，还要保护其来源的真实性和可用性，等等。如缺乏安全意识和必要的安全措施，使用这些设备可能导致信息被泄露、被修改、被破坏或错发错收，例如，在公共场合打移动电话可能将通话内容泄露，使用语音答录机时可能被偷听，对拨号语音邮件系统的未授权访问或使用传真机设备会偶然地将传真错发给别人等。

应当制定清晰的控制策略规定员工在使用语音、传真和视频通信设备时应遵守的流程，包括以下内容：

- 提醒员工不在公共场所使用电话谈论敏感信息，以避免信息被偷听或截获；
- 提醒员工不得在公共场所、开放的办公室或墙壁较薄的房间内谈论敏感话题；
- 不得在语音答录机上留言，因为这些设备可能被未授权人员盗听，或由于拨号错误而被录制到不该接收的地方；
- 提醒员工使用传真机可能导致的风险，例如：
  - 传真机内存信息被未授权访问；
  - 误将传真件发送到其他号码上，等等。

6.7　访问控制

对所有信息系统和信息服务最基本和最有效的安全控制措施是对信息系统资产(源)进行访问控制，这类措施应从访问主体、访问客体、访问路径和访问环境等角度考虑。

6.7.1　访问控制的策略

应对访问控制的需求进行定义并形成文档，对于每一个用户或用户组的访问控制规则和访问权限都应在访问控制策略文件中明确说明，对用户和服务提供商访问的需求必须根据业务流程进行配置。

制定访问控制规则应考虑以下内容：

- 不同业务流程的安全控制需求；
- 识别要特别保护的所有和业务应用相关的信息；
- 对信息实行分类保护的规则需求；
- 对于被访问的数据和服务进行保护的有关法规依据和合同约定；

- 特殊用户访问公共业务范畴信息的安全控制规程；
- 在分布式和网络化的环境中通过连接进行访问的权限管理。

制定访问控制规则还要进一步考虑以下内容：

- 区分具备一般条件即可执行访问的规则和需要附加条件才执行访问的规则；
- 一般情况下，控制规则应执行"未经允许都是禁止的"（默认禁止）的原则，而不是执行"未经禁止都是允许的"（默认允许）的原则；
- 信息标识（包括系统自动标识和由管理员标识）的变化引起访问控制判断条件的变化；
- 信息系统自动授予和管理人员授予引起的用户权限变化导致访问控制判断条件的变化。

6.7.2 用户访问的管理

制定正式的控制规程对用户访问信息系统和信息服务的权限分配进行管理，以防止对信息系统和信息服务的未授权访问和对用户访问权限的滥配或错配。该规程应该涵盖用户访问活动期的各个阶段，包括从新用户的注册开始到最后不再需要访问信息系统和信息服务时的注销等各个阶段。在需要分配专有的访问权限或允许用户越过系统控制进行访问时应进行特别的管理。

1. 用户注册

制定正式的用户注册和注销规程对多用户信息系统和信息服务的访问进行鉴别与授权。

用户注册规程应包括以下内容：

- 用户使用具有系统唯一性的身份标识符将用户和其访问行为联系起来，并使用户为其行为负责，只有在适合于群（组）工作方式的地方才允许使用组（群）身份标识符；
- 对用户访问信息系统或信息服务是否获得了系统管理者的授权进行审查，必要时，管理人员对访问权限实行特别许可也是需要的；
- 检查所授予用户的访问权限与业务的安全保护目标是否一致，并且是否和组织安全策略相一致，访问权限不可危害职责划分原则；
- 向用户颁发其访问权限的书面说明；
- 要求用户签署一个表明他们已理解访问控制条件的声明书；
- 确保只有在授权流程完成之后服务供应商才可以提供服务；
- 记录所有注册使用该服务的用户的正式名单；
- 对于工作岗位变动或离开组织的用户，应立即撤销其被授予的访问权；
- 定期检查和取消冗余的用户身份标识符和账号；
- 确保冗余的用户身份标识符不分配给其他用户。

应在员工聘用合同和服务合同中包括一些条款，对越权访问等违规行为必须承担的责任进行详细规定。

2. 特权管理

这里的特权指的是启动、关闭信息系统，遇到紧急情况时对信息系统或其子系统进行关闭，对信息系统运行必需的关键设备的初始化参数进行配置等重大操作活动所需具备的特

殊授权。这些特权一般只授予系统管理团队。具有这些特权不仅可拥有超越一般用户的操作权限,而且拥有对维持信息系统运行秩序的决定权。因此,对操作特权的分配和使用进行管理控制是信息系统有序、安全、健康和可靠运行的最基础性的管理活动之一。

信息系统应制定操作特权的授予和管理规程,对系统运行、维护、升级更新和紧急事故处理中所需的重大操作特权的分配、使用过程进行控制。特权管理控制规程应考虑以下事项:

- 建立与信息系统参数配置、正常启动、紧急处置和异常关闭有关的操作规程,将信息系统关键设备/设施(如操作系统、数据库管理系统和业务软件等)的操作特权分配给相应的系统管理员,对于大中型信息系统应将这些操作特权分别授予有关的系统操作员,对于某些重要信息系统中数据库管理系统的操作特权可分割给有关操作人员;
- 利用信息系统中的日志记录和审计与监控系统对所有系统操作人员的操作行为进行记录和监管;
- 对信息系统中所有操作权限的授予应遵循最小特权分配原则,也就是说,只给岗位角色授予他们在需要履行职能时需用到的恰当操作期限;
- 将授权过程和已分配特权的授予人、受授人名单记录在案。已被授予的特权未经批准不得变更或转授他人;
- 对信息系统重大设备初始运行参数的配置可使用供应厂商设定的账户和口令或维护端口,这些设备在调试结束投入正式运行之前应将供应商设定的账户和口令更改为新的账户和口令,并维持对维护端口的封闭;
- 经批准,信息系统操作人员可启用维护端口处理紧急情况或进行系统的例行维护。

3. 用户口令管理

口令是用户身份鉴别信息的一部分,常用来识别访问信息系统或信息服务的用户的身份。信息系统用户的口令可由系统管理员分配,也可由用户通过系统的界面生成并经系统验证后使用,对用户存于计算机中的口令进行保护是系统管理员的一项重要职责。对用户口令的管理措施如下:

- 用户签订口令保护承诺书,保证本人的个人口令未经批准不得以任何形式(包括通过网络和以口头方式)向他人泄露,以及所持有的组(群)口令只限于在组成员之中(这可以包含在雇用条款和条件中)交流;
- 分配给用户或用户自己按规程生成的口令应具有相当的安全性,并定期予以更新,用户丢失口令时由系统管理员在通过对用户身份进行确认后予以重新生成,并从系统中废止原来的口令;
- 必须通过可控的网络通道或密件方式传递口令,不得使用第三方通道或未受保护(明文)的电子邮件传递口令信息,用户对收到的口令要通过合适的渠道予以确认。

生成的口令应具有一定的抗猜测强度,存储在计算机中的口令应有某种形式的安全保护措施(例如对口令加密存储)。

其他用于标识用户身份的识别物,比如指纹、签名和硬件标记(如芯片卡),都可用于标识和识别用户的身份,其功能相当于用户口令,但安全性强于口令。

4. 对用户访问权的检查

为了对用户访问信息系统和信息服务的权限进行有效监管，管理人员应该对用户访问权进行检查：

- 对用户访问权限定期进行检查（建议 6 个月为一周期），并在变更后进行复核；
- 对特殊访问权的审查周期不长于 3 个月；
- 定期检查特权的分配和使用情况，以确保分配的特权不被滥用或盗用。

6.7.3 用户的安全职责

防止未授权或越权访问是信息系统有序、安全运行的基本条件，也是系统合法用户必须遵守的职业道德和安全责任，要求用户必须意识到自己在维护访问控制规则中的责任，特别是在用户口令的使用和维护过程中的责任。

1. 口令的使用

用户在选择和使用口令时应遵循安全规范。

口令提供了确认用户身份的一种方法，访问控制机制以此确认用户对信息处理设备的访问权。建议所有的用户：

- 保护口令不以任何形式泄露给他人；
- 避免将口令信息记录在纸上和信息处理设备上；
- 如有迹象表明口令受到攻击或有泄露的风险，应立即通过管理员更改口令；
- 选择字符足够长的、数字和字符混杂的高质量的口令，并尽量做到：
  - 不要使用与个人有关的信息作为口令，如名字、电话号码和生日信息，等等；
  - 不要采用连续是同一字符或全数字、全字母的口令。
- 定期或基于访问次数更改口令，特权账号的口令更换更要频繁一些，避免多次重新使用或循环使用口令；
- 第一次登录新系统后应立即将设备配置的默认口令更改为用户自己设置的口令；
- 不要把口令信息包含在任何自动登录的程序中，例如保存在宏或功能键中；
- 不与他人共享个人口令。

如果用户需要访问多项服务或应用平台软件，建议用户对所有服务使用唯一的高质量的口令；也可以使用硬件 ID 作为一卡通，进入应用平台后，再对信息服务采用一般口令进行访问，这些做法可能比使用多个质量不高的口令安全一些。

2. 对无人值守设备的管理

对无人值守的设备必须有周密的保护措施。在用户区安装的设备，如个人计算机终端、工作站或文件服务器，当长时间无人值守时，针对未授权访问的风险需要有特殊的安全保护措施。用户和承包商必须意识到保护无人值守设备的安全要求和流程，以及在实施这种保护时的责任。建议用户：

- 除非有适当的锁定机制（如屏保口令）保护，否则设备使用完后应终止活动的进程或予以关闭；
- 进程结束之后，应从主机上注销并退出系统，然后关闭个人计算机终端；
- 通过键盘锁或类似措施避免对个人计算机或终端的未授权使用，例如口令保护。

6.7.4　对网络访问的控制

对内部网络和外部网络之间的访问活动必须进行控制。为了确保外部用户访问内部网络及其信息或服务的行为不会危害到这些网络服务的安全性，要确保以下内容：

- 在组织内部网络和其他组织的网络以及公共网络之间有符合安全规范的隔离措施；
- 对用户和设备身份的真实性有适当的鉴别机制；
- 控制外部用户对组织网络和信息服务的访问。

1. 制定网络安全访问策略

用户只可以直接或间接地访问已获明确授权的网络系统或信息服务。对用户访问权限进行控制，特别是对于连接到敏感的或关键性的业务应用软件或通过高风险区（如在组织安全管理和控制之外的公共或外部区域）对内对外的连接的用户特别重要。

应制定有关使用网络和网络服务的安全策略，包括以下内容：

- 允许用户授权访问的网络和网络服务清单；
- 允许访问不同网络和网络服务的内部或外部用户获得授权的规程；
- 对网络连接和访问网络服务的管理控制规程。

2. 控制访问路径

应控制从用户终端到网络服务的通信路径。网络设计的基本出发点是允许最大范围的资源共享和路由的灵活性，但这种特点也给未经授权的访问业务应用软件和使用信息设备提供了机会。对用户终端和允许它们访问的网络服务之间的路径进行控制是减小访问风险的有效方法之一。

控制访问路径的目的是防止用户在用户终端和其已被授权访问的服务之间的路径以外选择路径，这需要在路径的不同节点上实施一系列的控制措施。其原理是通过事先选定的路径来限制在网络中每个节点上的路由选项。

3. 外部接入的用户鉴别

用户从外部接入网络可能对业务信息进行未授权的访问，如拨号方式的访问。因此，远程用户的连接访问必须经过身份鉴别。鉴别方法有不同的类型，一些方法可提供高安全级别，如基于加密技术的方法可提供很强的身份鉴别。通过风险评估来决定鉴别方法的选择原则。

对远程用户的鉴别可以使用（如基于加密技术的）硬件令牌或质询/响应协议来实现；专用线路或网络用户地址检验设备可以用来提供对连接源地址的鉴别。

对回拨过程进行控制，如使用回拨调制解调器可以防止对组织信息处理设备的未授权和不需要的访问。这种控制措施可以识别企图在远程站点和组织的网络之间建立连接的未授权用户。在使用此类控制措施时，组织不得使用含有呼叫转接的网络服务，因此，这些服务必须禁止使用呼叫转接功能，以避免由此带来的隐患。回拨过程必须保证在组织的一方可以主动中断连接，否则，远程用户可以保持线路的持续开放，而在第二次回拨时不必进行回拨鉴别，这是很危险的。对于这种可能的风险，要进行彻底的测试和评估。

4. 节点鉴别

计算机远程自动连接的功能可能留下未授权访问业务应用的隐患，因此对远程计算机

的连接要进行真实性鉴别。如果连接是由组织可控制范围之外的网络发起的，鉴别则尤为重要。节点鉴别可以作为一个可选方法，用来验证连接到共享的计算机设备的远程用户的真实性。

5. 远程诊断端口控制

对诊断端口的访问必须严格控制。很多计算机和通信系统都配备有供维修工程师使用的拨号远程诊断端口。这些诊断端口提供了不需授权且权限很高的访问设备的途径，因此必须严加控制。另外，应有适当的安全控制机制(如使用键盘锁、密封条和严格的管理规程)来确保只有计算机服务管理人员和要求访问的软/硬件支持人员在得到授权后才可以访问这些端口。

6. 网络隔离控制

从技术本质上讲，开放互连网络与外部网络之间没有物理意义上的边界，这正是建立业务合作关系所需要的。这种网络特性如不采取任何控制措施会增加对建立在网络上的信息系统进行未授权访问的风险，这就需要在内部网络和外部网络之间采取控制措施，以便既能进行业务合作，又能防范来自外部网络用户的未授权访问。

这里的内部网络和外部网络是一个相对概念，特别是外部网络可以是组织外的另一个组织的网络或公共网络(包括因特网)，也可以是大型网络中其他部门或机构的网络。

控制大型网络中部门网络之间和业务网络之间边界的一种方法就是把网络划分成若干物理的或逻辑的网络域，对每一个网络域所定义的边界进行控制保护。这种边界保护措施可以是在相连的两个网络域之间安装安全网关，或是通过对交换设备配置划分虚拟局域网(VLAN)，这都可以控制其间的访问路径和信息流，必要时还可以在两个安全域之间安装单向传输控制设备，以控制数据流向。

在组织内部网络与其他组织的网络或公共网络之间的控制措施可以是采用防火墙、交换设备或应用网关一类的逻辑隔离控制措施，也可以是采用摆渡式的网闸或单向传输控制设备。这两类隔离措施对信息流的控制方式是不一样的，前者是基于规则控制信息流，后者是基于硬件技术控制信息单向传输，因此隔离控制强度差别很大。

7. 网络连接控制

对于访问共享的网络特别是访问跨越组织边界的网络，需要制定访问控制策略，控制策略中必须包括限制用户连接类型的控制措施。这种控制措施可通过网关来实现，网关通过预先定义的路由表或路由规则来过滤通信连接。所实行的限制措施应基于业务应用的访问策略和变更需求进行维护和更新。

8. 网间的路由控制

共享的网络特别是扩展到组织边界之外的网络，需要用路由控制措施来确保计算机的互连和信息流不会违背业务应用的访问控制策略，对于和第三方(非本组织)用户共享的网络，这种控制措施是不可缺少的。

路由控制应具有对源地址和目的地址的审核机制，网络地址转换对于网络隔离和防止路由从一个组织的网络扩展到另一个组织的网络是一种很有效的机制，这种机制可通过软件和硬件形式实现，在实施时应注意到所采用机制的控制强度。

9. 网络服务的安全管理

大范围的公共网络和专用网络上的网络服务有很多种，其中有一些服务可给用户带来

增值效应。网络服务具有个性化的、复杂化的特点，使用网络提供服务的组织必须提供一个对所使用服务的安全规则的清晰描述。

6.7.5　对操作系统的控制

操作系统本身一般都提供一些限制对计算机资源进行访问的功能，但这些功能需要进行必要的配置才能发挥作用；此外，要更严格地防止对计算机的未授权访问，还需要从管理上利用操作系统提供的附加安全控制措施。这些措施应该做到：

- 根据计算机防范未授权访问的实际需要，在操作系统安装后立即对一些初始化运行参数的默认值进行修改，以适合本机运行的安全需要；
- 对访问计算机资源的任何实体（例如其他计算机用户、进程）的真实身份和来源进行鉴别，如有必要还应附加核对合法访问实体的访问权限的控制措施；
- 记录成功的和失败的对计算机的访问行为；
- 提供对计算机弱口令的审核，确保用户使用高质量的口令；
- 一般情况下，限制用户的访问频度或在一定时段内访问的次数，也可对未授权访问行为起到遏制作用。

6.7.6　对应用系统的控制

在应用系统（特别是业务应用程序）内应采取安全措施限制对应用程序或业务流程的访问，以防止对信息系统的信息和信息服务的未授权访问。一般的应用系统（某些匿名登录的公共信息系统除外）都有一些由产品生产商开发的访问控制措施，例如登录的账户和口令等，但这些措施在身份鉴别和访问权限控制方面的控制力度是否满足对信息和信息服务的机密性、完整性和可用性的保护要求可能存在问题，因此需要根据对信息和信息服务的保护措施进行评估的结果来判断。如果由生产商开发的应用系统的保护力度不够，则应该采取额外的控制措施。

对应用系统提供的信息和信息服务进行访问的范围必须限定在被授权的用户中。应用系统对未授权访问的控制措施应遵循以下原则：

- 依照定义的对信息和应用业务的访问策略控制对信息和信息服务系统的访问；
- 对所有可能超越应用系统控制的操作（例如利用工具对应用系统进行诊断的）特权予以识别，并从管理规程和技术措施上进行控制，防止操作特权的滥用；
- 对应用系统的信息和信息服务的访问不得危害共享信息资源的安全性；
- 明确制定具有合法访问应用系统权限的名单列表。

1. 对信息访问的控制

应该依照制定的访问控制策略，基于不同业务应用的需求，对应用系统用户（包括支持人员）提供访问信息和应用系统功能的权力。为支持对访问的限制需求，应考虑采取下述控制措施：

- 授权访问应用系统信息和信息服务的用户只能按系统提供的菜单进行操作；
- 用户只能访问被授权访问的信息和应用系统提供的信息服务；
- 控制用户对信息的访问权限，如读、写、修改和删除等操作；
- 应用系统的输出只包含与用户访问有关的信息，并只能发送到授权的终端和站点。

2. 对敏感应用系统的隔离

敏感应用系统可能要求有专用的(或与外网进行物理隔离的)计算环境,这就意味着这样的应用系统应在专用的计算环境中运行,只能与可信的信息系统共享资源。

6.7.7 监控

这里的监控指的是对信息系统内各种设备的运行状态以及发生在信息系统内的操作行为和通信事件的监视与控制,以发现计算机和网络设备的异常运行情况,以及违背访问控制策略的操作事件和通信行为。监控的目的是监测信息系统设备的运行以及未授权的操作行为和通信事件,以便在发生安全事件后提供责任证据。

通过对与监控有关的信息整合,还能验证所采用的控制措施的有效性和充分性。

1. 日志记录

日志记录是计算机和网络设备操作系统提供的,用于记录计算机和网络设备中发生的操作行为与通信事件。通过对日志记录的数据进行观察和整合形成审计日志,可以获得对信息系统中出现的可直接观察的或不能直接观察的操作行为和通信事件更深刻的理解,从而判断信息系统运行过程中可能出现的异常操作行为和通信事件。由这些异常情况可推知信息系统运行中出现的不可接受的事件类型(例如未授权访问、合法用户越权访问、用户违规访问和通信、信息和信息服务的可用性丧失等),并可为追究各种事件的责任提供直接证据或间接的线索。日志记录应包括以下内容:

- 用户身份标识符;
- 登录和退出系统的日期和时间;
- 计算机终端的身份和位置标识信息;
- 成功的和被拒绝的访问信息系统的尝试;
- 成功的对外连接或被拒绝的对外连接的尝试;
- 成功的和被拒绝的对信息和信息服务的访问尝试。

可靠的日志记录应作为信息系统运行档案的一部分,一方面为审计提供原始数据,另一方面供事件后的深入分析使用。

2. 监控

应建立监控信息处理设备使用情况的流程。为确保用户只进行被明确授权的操作,这些流程是必需的。对不同设备所需的监控强度应根据风险评估来确定,应该进行监控的对象如下:

- 授权访问,包括以下细节:
  - 用户 ID(身份标识符);
  - 操作事件发生的日期和时间;
  - 事件类型;
  - 被访问的文件、使用的访问程序和设施。
- 特权操作,例如:
  - 使用系统管理员账号;
  - 系统的启动和关闭;
  - 输入/输出设备的连接与断开。

- 未授权的访问尝试，例如：
  - 访问失败的操作实体及重复尝试的次数；
  - 对网关和防火墙等访问策略的违背和告警；
  - 入侵检测系统报警。
- 系统警报或故障，例如：
  - 控制台（信息系统管理器界面）警报或消息；
  - 系统登录异常及告警；
  - 网络管理警报。

对日志记录的审查包括了解系统的脆弱性及其面临的威胁和威胁发生的形式。

系统日志记录通常包括大量的信息，其中有很多和安全监控无关。为帮助辨认出对安全监控目的有意义的事件，应考虑将消息进行适当分类，并自动复制到第二层次的日志中，或使用适当的记录设施或工具执行文件审查工作。这些工作对日志审计和事件的深入分析极其有用。

担任日志审查的人员不得兼任信息系统操作员，并与被监督人员的角色分开。

3. 时钟同步

计算机信息系统时钟的正确设置对于确保日志审计结果的准确性极为重要，因为这些日志是调查所需要的，或是法律事件、违规事件的责任证据。不准确的时间会妨碍调查和影响作为证据的可信性。

在计算机或通信设备有能力运行网络时间协议（NTS）的情况下，有条件的信息系统要使用网络时间协议系统。时钟应被设置成公认的标准时间体系，例如世界协调时间（UCT）或当地标准时间。如未能安装网络时间协议系统，为防止时钟随时间出现的漂移偏差，应制定规程来检查和修正出现的明显时间偏差。

6.7.8　移动计算和远程接入控制

移动计算设备的远程接入可经由第三方服务提供商在远程现场实现，也可以经由自己控制的无线网络实现。一般地，移动计算设备远程接入的目的都有通过组织外网络或公共网络连接到其所属组织信息系统访问信息和信息服务的需要。维护远程接入的安全需要一系列的规范操作，如通过第三方远程接入服务商实现远程连接，则服务商必须承担远程接入点的安全维护责任；如使用自设无线网络连接，则需进行风险评估，目的是确保移动计算设备通过远程连接到组织的信息系统的整个过程的信息的机密性、完整性和可用性。

维护安全的远程连接需要注意下列事项：

- 确保组织对无线网络运行的控制权；
- 对投入运行的无线网络和移动计算机设备进行标识；
- 移动设备在接入无线网络前应进行身份鉴别，必要时进行双向身份鉴别；
- 应用补丁和安全增强技术维护无线网的安全；
- 如使用第三方服务商实现远程接入，则应与其签订安全保护协议；
- 如通过第三方接入，最好对连接过程中处理的信息进行加密保护；
- 为防范未识别的脆弱性和威胁，对接入网形成的风险必须加强监控；

- 移动计算设备本身如涉及国家秘密，未经批准一律不允许通过第三方远程接入提供商的信息系统。

当前基于互联网技术的通信协议和商业产品所提供的保护措施对组织的移动设备使用远程接入来说，其安全性是不充分的。使用第三方服务的远程接入可能引入一些不可接受的风险。在部署无线接入技术之前，代理商应主动识别其中的风险，并采取安全防范措施。此外，很多组织在管理自设的无线接入系统方面还存在安全意识不强或技术素质不够的问题，例如对生产厂商的默认配置不加分析地接受，或对入口控制点不提供合适的安全保护机制，也没有配置适合无线网络环境的安全保护设备（例如在有线网络和无线网络系统之间配置防火墙、阻断不需要的服务/端口、使用加密技术等）。在大多数情况下，大部分风险是可以通过施加安全措施减小的，不过也要考虑减小风险所花费的代价与所获得的安全效能之间的平衡。

1. 移动计算

在使用移动计算设备（如笔记本计算机、掌上电脑和移动电话）时，必须确保业务信息不被泄漏，应重视使用移动计算设备带来的风险，并制定适当的保护策略，特别是在未受保护的通信环境中。这些保护策略应包括对其进行物理保护、访问控制、数据加密、备份、病毒防护的管理和控制规程，以及移动设备接入业务网络的安全规则和方案。

在会议室和组织网络边界之外的其他未受保护的地区使用移动计算设备时，应采用加密技术等对这些设备存储和处理的信息进行保密，避免未授权访问或泄漏。

对于连接到组织外网络上的移动设备，不管是用于办公还是跨过公共网远程访问业务信息都需经过鉴别，并有适当的访问控制机制。

对移动计算设备在办公或运输途中应强调物理保护，以防止被盗或遗忘在交通工具、旅馆房间和会议室里。承载重要的、敏感的或关键性的业务信息的移动计算设备必须由专人照管，并不得人机分离。如有可能，应进行物理锁定，或使用特殊的掩护方法来保护设备。

加强对持有移动计算设备的员工进行安全意识和技术素质的培训，提高他们对这种工作方式所引起的额外风险的意识和采取保护控制措施的意识。

2. 远程接入

远程接入是利用网络通信技术使员工在组织之外的异地或系统外接入本地网络，并访问组织内的信息资源。在远程接入站点要防止非授权的信息泄露或对设备的滥用等。

组织应对远程访问活动制定严格的信息安全控制策略，这一策略必须遵从组织的安全策略。只有在组织的信息安全控制策略下采取了必要且充分的安全保护与管理措施，才可以允许对组织的业务系统进行远程访问。在采取安全保护和管理控制措施时，应考虑以下因素：

- 远程接入站点的物理安全应当满足建筑物和环境的物理安全标准；
- 远程接入站点的接入供应商应承诺对接入设备内和通过接入设备的信息不截获、侦听或外泄；
- 远程数据应通过安全通信通道或安全协议传输；
- 通过远程接入的计算设备不得越权访问组织的信息系统的信息和信息服务。

远程接入的保护和控制措施如下：

- 对远程接入的设备和存储工具必须经过身份鉴别；

- 规定远程访问活动的操作时间以及远程设备授权可访问的内部系统和服务资源；
- 约定使用远程移动计算设备的类型和远程访问的操作流程；
- 远程接入设备与组织的业务系统之间交换的数据通过安全隧道传输，传输敏感信息时还应对数据进行加密；
- 加强对远程接入设备和访问活动的监控与审计；
- 远程接入访问活动结束时，撤销对远程移动计算设备从远程访问组织的信息系统的授权。

6.8 系统开发和维护

6.8.1 系统的安全需求

此处所说的系统是指完成业务的应用信息系统。在开发信息系统的应用(或服务)的业务流程之前，应先与项目需求分析一起对其中需要解决的安全保护和管理问题进行识别并予以确认，这就是信息系统安全需求的开发问题。

安全需求是针对信息系统的应用(或服务)的业务流程在其存活期间的风险应对策略。由于信息系统的资产存在脆弱性，可能面临来自系统内部或外部的威胁，这些威胁的主体(即执行者)在一定条件下可能成功地利用或开发脆弱性，从而对信息系统的某些资产或系统整体在机密性、完整性和可用性等方面造成损失(害)或负面影响，对信息系统构成风险。

特别需要提醒的是，这里所说的应对风险的策略还应包括将对安全需求的陈述转化成具体的安全保护和管理的措施，因此安全需求和安全措施之间是直接关联的。例如，通过公共网络环境传输敏感信息时，由于传输线路存在电磁泄漏或可物理接近的脆弱性，因此面临无线窃听和搭线侦听的威胁，这就可能形成敏感数据被窃取或外泄的风险；应对此类风险的安全需求即是要求传输线路防电磁泄漏和物理不可接近；为满足安全需求，在安全保护措施上采取光缆通信，尽量降低电磁泄露，通信线缆外加较为坚固的管道(在可能的地方采用地下管网)防范搭线窃听，必要时对传输的敏感信息进行加密，同时在管理措施上加强监控和通信保护条例的宣传教育。

所有的安全需求应当在项目需求分析阶段被识别出来，并论证其必要性和充分性，然后文档化，作为信息系统整体文档资料的一部分妥善保存，并随着项目需求的修改或变动进行更新。最终审定的安全需求将转化成具体的信息安全保护措施(技术性措施，如设备、设施和软/硬件模块等；管理性措施，如建立规章制度和操作规程等)供选择和配置。

由安全需求转化的安全保护措施应当体现所保护的信息资产的价值，以及可能由故障或安全措施的不充分或缺失而存在的潜在业务损失。由于安全保护措施的不充分或缺失而存在的风险是信息系统残留风险分析和评估的主要内容。

在信息系统的应用或在服务业务设计时就引入安全需求分析，进而对安全保护措施的效能进行评价，比在实施中或实施后再针对安全问题引入安全控制措施，其整体安全性及其安全效费比更为优化和合理。

6.8.2 业务流程安全

在开发设计应用业务信息系统时，应当对业务处理流程的安全保护做出安排，并在业务

处理流程中插(嵌)入适当的安全控制机制。这包括书面的业务流程的操作规程,对处理流程中的输入数据、内部处理流程和输出数据的确认机制等,目的是防止丢失、修改或误用应用系统中的用户数据。

对于处理敏感的、有价值的或重要的组织资产的信息系统可能需要额外的安全控制措施,这样的安全控制措施应当根据安全需求来确定。

1. 输入数据的确认

输入应用系统的数据应当确保它是系统需要的和符合规则的。

应当考虑下列控制措施。

- 采取措施检测下列错误:
  - 数据长度超过规定的位数;
  - 数据字段中包括无效字符;
  - 丢失的或不完整的数据;
  - 超出数据量的上、下限制;
  - 未授权的或不一致的控制数据。
- 检查关键字段或数据文件的内容,以确定其有效性和完整性;
- 通过检查所复制的输入文档,判断输入文档是否存在未授权的变更(对输入文档的任何变更都应当经过授权);
- 对输入错误予以响应的操作规程;
- 测试输入数据合规性的操作规程;
- 记录数据输入过程中所涉及的所有人员及其操作。

2. 内部处理的控制

已正确输入的数据可能因为内部处理错误或故意的行为而被破坏,应当在应用信息系统的业务流程中插入检测模块,对处理过程中合法数据出错的情况进行识别。应用信息系统软件的设计应当将导致数据完整性丧失的软件缺陷的风险降至最低,这类风险包括:

- 在应用程序中设置增加与删除功能可能导致非法或越权对数据的变更;
- 应用程序的缺陷导致业务流程以错误的逻辑顺序运行或在故障修复前继续运行;
- 故障恢复处理规程存在缺陷。

业务流程内部控制检查的项目和内容取决于应用业务信息系统的性质以及数据受到破坏后对业务的影响,其检查实例可能包括:

- 会话或批处理控制措施;
- 系统生成的数据的确认流程;
- 中央计算机和远程计算机之间下载和上传数据或软件的完整性保护机制;
- 记录数据和文件数据的完整性保护机制;
- 应用程序运行的逻辑顺序是否存在缺陷,能否在出现故障时停止运行,并在故障修复后恢复运行。

3. 消息鉴别

消息鉴别是一种完整性保护机制,可用于检测传输的电子消息的未授权变更或破坏。它可以通过支持物理消息鉴别装置或软件算法的硬件或纯软件实现。

应当考虑采用消息鉴别技术保护消息内容的完整性,例如对非常重要的电子资金划拨

或其他类似的电子数据的交换进行完整性检测。对应用系统的业务特性和处理流程进行安全风险评估可以帮助决定是否需要采用消息鉴别机制。

消息鉴别并不是设计用来保护消息的内容免受未授权的暴露的,但加密技术在保护消息不受未授权暴露的同时,却可以用来实现消息鉴别。

4. 输出数据的确认

对从应用系统中输出的数据应进行确认处理。对输出数据的确认处理包括:

- 制定输出数据合规性测试的规程;
- 使用规程测试输出的数据的合理性;
- 使用一致性的计算方法控制所有输出数据在处理方法上的一致性;
- 记录数据输出过程中所涉及的所有人员及其操作。

6.8.3 加密控制

对于面临泄露或暴露且用其他的控制措施不足以保护的(数据)信息,应当使用加密技术来保护信息的机密性、真实性或完整性。

1. 使用加密控制措施的策略

使用加密方案保护数据是在评估风险后选择的一种保护控制措施。在通过风险评估结果决定的安全保护措施中,加密保护控制措施是在采用其他措施仍不足以或不能够达到安全需求规定的保护强度的情况下的措施。加密技术方案不仅能保护数据的机密性(不被泄露、不可访问或不可理解),而且能保护数据的完整性(不被修改,或在遭受修改后恢复),以及验证数据的真实来源。但加密保护措施花费的投入和运维更多,成本较高,因此最终确定使用哪种类型的控制措施应综合考虑多种因素,不可盲目地追求加密保护措施。

一个组织应制定一个完整的使用加密控制措施的策略。为了获得安全保护的最佳效费比,并将使用加密控制措施的风险(例如滥用密码、密钥丢失等)最小化,制定密码使用策略是必需的。在制定这种策略时,应当考虑以下事项:

- 组织使用加密控制措施的管理方案,包括法律遵从性、数据加密保护等级、密码类型、数据保护范围等;
- 密钥管理方案,包括密钥种子、密钥生成、分发、注册、使用、注销,以及在密钥丢失、泄漏、被破坏情况下的应急处理方法;
- 密钥管理与使用的角色及其应承担的责任;
- 对加密实施过程的管理控制;
- 密钥管理系统的维护规程。

2. 密码技术管理

加密技术是一种数据变换技术,其使用应当遵循上述策略原则,切不可滥用,因为不适当地使用密码加密技术或对密码系统管理不当也是有风险的。

应当根据风险评估综合考虑采用的加密算法的类型和质量以及所使用的密钥的长度,与所保护的信息数据的安全等级需求相适应,过度保护和欠保护同样是有害的。

在决定采用加密技术保护信息系统数据时,一个重要的问题是不同国家(和地区)对使用加密技术的法律限制可能不同(甚至差别很大),因此要考虑加密信息跨国界流动可能遇到法律障碍,进而造成技术性障碍。此外,如果未经批准引进国外加密技术和设备,不仅违

反法律规定，而且由于密码核心技术受制于人，从数据保护角度来讲最大的风险如同用来保护数据的保险箱的钥匙实际上在货主或保险箱生产商手中一样。

密码技术问题应当寻求专家的建议，密码使用的法律问题应当咨询国家密码主管机构。

3．数字签名管理

数字签名技术是密码应用技术的一种，用于保护电子文档完整性和来源真实性。

数字签名适用于电子化处理的任何形式的文档，例如签署电子支付凭证、资金的划拨、合同和协议等。这种技术使用私钥生成签名，而使用公钥验证该签名。因此应当注意保护私钥的秘密性，因为任何能够窃取别人拥有的私钥的人都能够假冒他人签署文档，例如支票、合同；同样，通过对公钥的鉴别技术保护公钥的完整性也是很重要的。

在考虑使用数字签名技术时，需要考虑所使用的签名算法的类型和质量，以及所使用的密钥长度，与被保护数字文档的安全等级要求相适应，过度保护和欠保护都是有害的。

在使用数字签名时，同样应当考虑法律限制，特别是在电子商务中，了解数字签名的法律有效性是很重要的。

4．抗抵赖服务的管理

抗抵赖服务用于解决信息收发双方对于收发信息的操作行为的否认，以及对收发信息的内容出现的争执。这种安全服务在电子商务合同或支票来往中是最为常见的，也是解决由于当事人有意无意的行为造成的争端或由于线路故障出现的传输错误导致的争端的最有效的方法。

这种安全服务形式可由相互信任的双方约定解决争端方式，也可经由双方信任的第三方对出现的争端进行仲裁。

对于前一种解决争端的方式，信息收发双方应约定采用数字签名技术来保证信息的收发双方身份的唯一性，以及对收发的信息内容的不可更改性，并对信息传输过程中可能出现的数据差错采取校验和纠错措施。显然，在这种方式下双方对于签名用的私钥必须妥善保存，而且需要约定在私钥被泄露或丢失的情况下的应急处置方案。对于后一种解决争端的方式，第三方的公正性和可信度是必须首先考虑的因素。需要制定双方都可接受的选择第三方仲裁机构的规程，以及对第三方机构必须遵守保密协议的约束机制，防范第三方侵害合约双方利益的风险。不过，即使通过第三方提供抗抵赖服务，在数据收发双方附加使用数字签名技术仍是一种可选择的抗抵赖的好方法。

5．密钥管理

密钥管理对确保加密技术的有效实施、防范密钥泄漏或丢失以及滥用密码技术等风险都是极为重要的基础性工作。在我国，密钥管理体系已有技术规范，规定了从密钥种子产生到密钥生成、分发、注册、使用、注销和作废的整个过程的技术标准。

决定采用加密方法保护信息数据的组织除需要遵从法律性规定履行审批手续外，必须配备符合技术规范的密钥管理系统。

应当保护所有的密钥防止修改、丢失和泄露。加密技术也可以用于保护密钥本身，而物理保护方法则可以保护生成、存储的密钥和将密钥存档的设备。

为了降低密钥泄漏的风险，密钥应当规定使用的有效期和失效期，即密钥仅在一段有限的时间内是有效的。密钥有效时间段的长短取决于加密措施适用的环境以及系统面临的密码破译风险。

6.8.4　开发进程对变更的管理

应当严格控制项目的开发环境和支持环境，维护应用系统软件开发的信息安全。

负责应用业务系统的管理人员也应当负责项目开发或支持环境的安全，他们应当对开发进程中的变更进行审核，以确定不危害系统或操作环境的安全。

1. 变更控制流程

为了将应用系统软件的缺陷和漏洞降至最小程度，应当对应用软件系统的变更进行严格的审核控制。为此，应当制定软件系统变更的控制流程，并对控制流程的执行进行监督；如需修改控制流程，必须经过论证，并得到批准。

从事技术支持的程序员只能访问软件系统中与他们的工作有关的那些部分，如需对所访问的部分进行变更，则应当在之前获得对拟做变更的正式批准，并将变更后的软件副本和有关变更的书面说明提交给系统管理人员。对应用软件的变更可能要求对操作规范进行同步变更。对变更过程的管理措施如下：

- 制定一个应用软件系统变更的授权规程；
- 制定应用软件变更流程，定义应用系统软件内部各子系统之间对变更的响应措施；
- 识别所有需要修改的计算机软件、信息、数据库和硬件；
- 在变更开始之前获得对详细变更方案的正式批准；
- 确保授权实施变更的人员接受变更方案；
- 将变更过程中信息服务流程受到的损失最小化；
- 确保在完成每次变更之后建立更新后的电子和纸质的完整文档，并将新、旧文档分类存档；
- 确保变更的软件版本是由获得授权的人员提交的；
- 保持对所有软件更新的版本控制；
- 保持对所有变更请求的跟踪监管；
- 确保用户操作流程随软件系统的变更同步变更；
- 确保变更后的软件系统在运行中不引入新的不可接受的风险，不对应用业务的持续性产生过大影响。

组织的应用信息系统应当维护一个测试新软件的环境。该环境与开发和生产环境相互隔离，测试人员与开发人员、生产人员和运行人员之间的职能不相互交叉，这是对新软件变更进行控制的必要措施之一。

2. 对操作系统变更的技术检查

有必要定期变更操作系统。对于现实应用的主流操作系统，所谓的变更是版本更新和在同一版本下安装补丁程序。当操作系统发生变更时，应当检查和测试应用系统对操作系统的适应性，以确保对软件应用系统的操作程序没有产生负面的影响。检查和测试过程应当包括以下内容：

- 测试新版操作系统或在安装补丁程序后不引入新的脆弱性，必要时这一测试工作应由国家指定的有能力的第三方机构进行，并给出负责任的检测报告；
- 检查或测试应用系统软件的运行没有受到操作系统变更的损害；
- 组织应做出年度安排，提供由操作系统变更所导致的检查和系统测试所需的人力和

财力资源；

- 提前向组织内与合作方有关的人员通告操作系统的变更事宜，以便在实施变更之前进行现状检查；
- 在对操作系统变更的同时，对业务持续性计划进行必要的变更。

3. 软件包变更的管理

一般不主张对购置的商业软件包进行修改，因为销售商不支持对所提供的软件包进行修改，原因有很多，但都很简单，其中的一个原因是商业利益和版权保护。其实，商业化的软件包应当是由具有相当技术能力的团队开发的，一般信息系统的程序员很难改得更好。但也存在某些特殊情况的确需要修改软件包，这时除需要得到供应商的技术协助外，还应当注意以下管控措施：

- 尽可能获得销售商的同意或技术指导；
- 对的确需变更的内容和方法进行充分论证；
- 在变更实施过程中，不得损害软件包内置的控制措施和程序调用过程，以免引发调用障碍或新的安全漏洞；
- 对变更后的软件包进行测试，并确认所变更部分没有出现新的安全漏洞，也不影响未被变更部分的功能，之后才能投入使用；
- 对由于软件包的变更引起的应用软件系统的业务流程变更可能造成的负面影响进行风险评估，如评估结果出现不可接受的风险，应重新考虑变更的内容或方法；
- 将所有的变更形成文档，以便在必要时作为原版软件的升级版本。

4. 隐蔽信道和特洛伊代码

隐蔽信道是两个进程共同以违反计算机信息系统安全策略的方式完成特定通信任务的一种方式，实际上并不是一般意义上的通信信道。例如，一个进程直接或间接写一个存储地址，而另一个进程直接或间接读该存储地址；有时一个进程的操作掩护另一个进程的操作，有时一个进程向另一个进程传递数据，或相互之间传递数据。隐蔽信道的目的是以一种隐蔽方式传输信息，以及在隐蔽信道中嵌入恶意代码，例如通过改变计算机系统中某些部件的访问参数达到非法访问的目的，或通过将恶意代码嵌入信息流中送入计算机信息系统，然后将其激活。

特洛伊木马程序是一种被设计成不易发现，但又不是信息接收者或用户所需要的代码，对系统进行非法操作的程序。隐蔽信道是传送特洛伊木马程序的通道之一，特洛伊木马程序则是具有某种功能的可执行程序。隐蔽信道和特洛伊木马都不是疏忽大意或系统缺陷所能为的，而是一种人为的故意行为。在那些担心隐蔽信道或特洛伊代码的地方，应当考虑以下措施：

- 从信誉好的供应商处购买正版软件；
- 购买程序的源代码，以便可以验证；
- 使用评估过的产品；
- 在启动使用前检查所有的源代码；
- 源代码一旦被安装，必须严格控制对源代码的访问和修改；
- 使用具有识别进程和恶意代码的检测工具，对未经允许的进程和恶意代码予以清除；

- 对操作关键业务应用系统的员工加强技术培训和职业道德教育。

5. 外包软件开发的管理

组织在决定将信息系统中的某应用业务软件委托给组织外的开发商进行开发时，应当考虑以下控制措施：

- 与具有技术开发能力和有良好社会信誉的服务商签订软件开发的委外合同；
- 确认最终软件产品的所有权和知识产权；
- 审查开发商提供的证明其服务资质和能力条件的资料的合法性和充分性；
- 规定对开发过程的质量和进度进行控制的方法，并确定具体负责人；
- 以与合同具有同等法律效力的附件形式对开发的源代码的质量指标予以详细列表说明；
- 确保组织与外包方对所需开发的软件的功能/性能需求有充分的、一致性的理解；
- 约定开发过程中解决纠纷的沟通机制，并指定联络人；
- 明确规定双方在软件外包开发中的安全管理责任；
- 在外包软件验收和安装之前委托具有资质的第三方对所开发软件进行系统性测试，并对软件缺陷进行专业的渗透性测试；
- 制定所开发软件经试用后的验收规程。

6.9　业务持续性管理

为了维持业务持续性，应通过(对系统、组件和各类数据)实施备份和灾难恢复计划相结合的模式，将灾难和安全事件引起的业务中断和系统破坏减少到可以接受的程度。

应当对灾难、安全事件和服务中断的后果进行评估，制定和实施突发事件应急计划，以确保被中断的信息服务流程可以在预期的时间期限内恢复。应急计划应成为整个信息系统管理过程的重要组成部分。

业务持续性管理还应包括识别在此之前遗漏的和新出现的风险，经过评估和论证后提出处置这类风险的策略建议。

1. 分析业务持续性中断的影响

从识别可能引起业务过程中断的事件(如设备故障、自然灾害和安全事件等)开始进行风险评估，以确定引起业务中断造成的影响(根据破坏的规模和恢复的时间判断)。这些活动的开展应由与业务持续性过程有关的所有人员普遍参与。

应当根据风险评估的结果制定安全需求计划，以决定维持业务持续性的总体策略。安全需求计划在制定后应当得到管理层的认可。

2. 制定和实施应急处理计划

应当制定计划，以便在关键性部件出现故障或系统遭遇不可预期的突发事件(包括安全事件、灾害事件等)引起业务过程中断后，在可控范围和预定时段内恢复业务系统的运行，因此对各种事件引起的局部业务中断和系统整体运行中断做出紧急响应是业务持续性计划的核心内容。应当考虑以下管理措施：

- 设立应急事件处理工作机构，确定应急事件处理所应达到的目标及策略原则；
- 制定一个信息系统中所有员工一致遵循的应急事件处理流程(包括局部应急处理和

系统整体运行的应急处理)，规定处理流程中的岗位责任及相应的监管机构；

- 制定应急事件处理的启动规程；
- 将应急事件处理的启动规程和处理流程制成标准化文档；
- 对与信息系统有关的人员进行应急事件管理的技术培训，培训内容因岗位而异，但必须使所有人员认识到自己的岗位在整个处理流程中的地位与作用以及与其他岗位之间的关联性；
- 对应急事件处理流程要进行测试和实战演练；
- 监控业务持续性过程，业务流程如发生变更，则应急事件处理流程也要变更。

3. 业务持续性计划框架

业务持续性计划包括提供不间断的信息和信息服务的过程管理、系统局部故障的识别和处理、系统服务中断的紧急处理，以及各种突发事件的应急处置和业务恢复等。维护这样一个独立的业务持续性计划框架可以保证所有计划实施的一致性以及测试和维护计划的优先顺序。对于业务持续性计划中的每一部分都应当明确规定执行的条件以及执行的负责人。当业务持续性计划出现新的变化时，应当修正已建立的应急处理流程。建立业务持续性计划框架应当考虑以下内容：

- 制定完整的提供不间断信息服务的过程管理规程，包括对业务服务系统从正常启动到整个系统运行过程的管理和维护，以及系统出现异常的常规性处置，直到关闭系统的所有操作规范；
- 预设启动各类应急处理计划的条件，这些条件描述每一个计划在启动之前所应判断的技术性指标；
- 应急事件处理流程应描述在相应的事件发生后，应由哪些操作岗位的人员采取哪些操作及这些操作应遵守的逻辑顺序，某些大事故和事件后的应急的事件处理流程还要包括公共关系的管理安排，特别是与公安机关、消防队和当地政府等的有效联络规范；
- 财产转移计划是应急处理流程的组成部分，描述在特别紧急的情况下将业务活动或支持服务必需的最小集软/硬件信息系统转移到预备的临时位置，为向必要的服务对象恢复服务提供物质条件；
- 恢复流程是应急事件处理的核心部分，描述将中断的业务系统恢复到正常的业务运营状况必须采取的一系列操作及操作顺序；
- 系统维护计划规定如何和何时测试业务持续性以及维护该计划的定期或不定期安排；
- 安全意识教育和技术培训计划是业务持续性计划的组成部分，对信息系统的有关人员理解业务持续性计划并自觉执行操作规范做出安全意识教育和技术培训的规划；
- 职责规范描述执行各部分计划的执行人和主管负责人，对业务持续性计划执行总责任人及关键部分计划执行人应当指定候选人。

对于每部分计划都应当配备一个特定的负责人。应急流程、转移流程和恢复流程的责任应当划入相应的业务资源或有关的业务过程的负责人的责任范围之内。对于技术服务的安排，诸如信息处理和通信设施等的技术支持，通常应当是服务供应商的责任，但组织应在采购合同中约定其维护或支持责任，并确定联络责任人。

4. 测试、维护和重新评估业务持续性计划

1）测试计划

业务持续性计划在测试时可能出现失败，这常常是由于不正确的条件假定、疏忽大意或人员变动造成的。应当定期测试业务持续性计划，以确保它们是最新的和有效的。负责系统恢复的所有成员以及其他有关的员工应参与和理解测试计划。

业务持续性计划的测试时间表应当指明如何以及何时测试计划的每个部分（直到计划中的所有部分），建议以遍历方式经常测试计划的各个部分，包括：

- 对不同应急处理方案进行桌面测试（通过使用业务中断实例来探讨业务恢复安排的合理性和实用性）；
- 模拟训练（尤其指培训事故或紧急情况之下，担任管理职责的人员的操作规范，并检验应急方案的合理性和实用性）；
- 对恢复计划中的实施措施进行测试（假设一个恢复实例，对实施信息系统的快速恢复能力及适应性进行测试）；
- 在备用的站点测试恢复流程（在远离主站点的场所进行系统恢复操作，同时进行业务处理）；
- 测试供应商的设备和服务（确保外部提供的服务和产品符合合同的承诺）；
- 完整的演练（测试组织、员工、设备、设施和业务过程在服务中断的紧急情况下的应对策略和措施的合理性、实用性）。

2）维护业务持续性计划

通过定期的检查和更新来维护业务持续性计划是确保业务持续性计划的有效性的管理措施。如发现存在某些业务安排应当却没有反映在业务持续性计划的情况，应在该计划的更新中安排进去。对变更的控制策略应包括对业务持续性计划的变更管理，对变更的管理包括新设备、操作系统的升级以及下列变动：

- 人员；
- 地址或电话号码；
- 业务提供策略；
- 场所、设施和资源；
- 法律法规；
- 承包商、供应商和主要客户；
- 操作顺序（或增加一些、取消一些）；
- 风险。

通过对上述与业务持续性运营有关的要素发生的变动进行跟踪，识别出与变动有关的影响，在经风险评估后采取有针对性的应对措施，是维护业务持续性计划的基本要求。

6.10　约束与限制

6.10.1　遵从法律性规定

在信息系统设计、（开发）实施、运行、维护和报废等各个阶段的管理中必须遵从法律、法

规和合同的规定要求，避免触犯所在国法律（包括刑事、民事）、法规而引起纠纷或诉讼，以及违反合同约定的赔偿责任。

1. 法律适用性

对于信息系统适用法律、法规的正当性描述以及有关合同约定条款的法律性依据应该制定成标准文档。为满足相应的法律、法规要求而采取的具体的控制措施和对应的个人责任也应明确地予以说明，并制定成标准文档。

2. 知识产权

1）版权

在使用与知识产权（如版权、设计权、商标权）相关的资料时，应确保符合法律（包括国际版权保护公约）规定。侵犯版权的行为可能导致民事，甚至刑事诉讼。

法律、法规和合同的要求可能限制对有版权资料的复制。在某些情况下，法律、法规可能规定只有组织自己开发的或者取得了许可证的开发者提供给组织的资料才能使用。

2）专用权

专用软件产品通常在接受许可协议下才能使用，并限制在特定的计算机上使用，且要求专用软件的复制品只能用于备份，应当考虑下面的控制措施：

- 制订获得正版软件产品的管理流程；
- 制订正版软件的使用规范，保证正版软件产品只在合法范围内使用；
- 提高保护软件版权和获取策略的自觉意识，认识到违反规定可能给自己和组织的信息系统造成严重后果；
- 保证拥有软件许可权的证据；
- 确保只有授权的软件和取得许可证的产品才能在系统内安装；
- 制定从公共网络（付费和免费）下载的软件运行于系统内部计算机的控制规程；
- 加强对组织获取的正版软件使用的监控。

3. 保护组织的记录文档

组织的重要记录文档应该得到妥善保护，以防止泄露、丢失、毁坏和篡改。就像支持基本业务活动的安全保护一样，记录文档也需要得到充分的安全保护。典型的记录文档例子是一些被作为证据的原始记录，可用于证明组织的运营是遵守法律法规的，或者在发生民事、刑事诉讼时，作为呈堂证供，或者供股东、合作伙伴和审计人员确认组织的经营状况。记录文档的保存时间遵从国家的法律、法规规定。

记录文档可划分为不同种类，如财务记录、数据库记录、交易日志、操作日志和审计日志等。每一种记录文档都应按保存期限选用合适的存储介质（如纸、缩微胶片、磁介质、光介质等）。在选择适合存储记录文档的介质时应考虑维护周期及成本。

一旦选定存储介质，处理规程应确保在整个保存期间对数据具有可访问性（存储介质和存储格式的可读性），防止由于技术变化造成数据（格式不兼容）的不可读。

选择的数据存储介质应保证以法庭可接受的方式进行读取或显示。

数据存储和处理系统应该明确地标记出所记录的类型和内容，以及法律、法规所要求的保存期限。在保存期届满后，如果组织不需要这些记录文档，应该以符合规范的方式由组织自己或委托第三方予以彻底销毁。

为了实施上述控制措施，以下步骤应该在组织内采用：

- 在合适的范围内公布保留、存储、处理和处置记录文档与信息的操作规程；
- 定期或不定期维护关键信息资源的存储介质；
- 采取恰当的安全控制措施保护重要的记录数据和信息不被泄露、丢失、损坏和篡改。

4. 数据保护和个人信息隐私

对涉及个人的数据的采集和传送应依法进行保护。这类保护措施可能对收集、处理和传播个人信息设置限制，并且对将个人信息从一个国家传递到另一个国家设置限制。

保护组织的数据需要依法采取适当的管理控制措施。通常，最好的做法是任命一个数据保护专员，制定针对管理者、使用者和服务供应商的个人责任和应该遵守的特定控制流程。

5. 防范滥用信息处理设备

组织的信息处理设备是为了实现业务目标而提供的，管理层应该对信息处理设备的使用进行授权。在没有得到管理层的同意时，任何出于非业务或非经授权目的而使用信息处理设备的行为都应该被视为不适当的或滥用设备的行为。如果这类行为通过监控或者其他途径被确认，应该引起管理者的注意，并考虑对此进行适当的调查或惩罚。

使用监控措施的合法性因国家的法律规定而有所区别，并且可能要求事先通知员工或者得到他们的同意。一般情况下，在实施监控措施前应具有法律许可（包括法律不禁止）的依据。

许多国家已经制订或者正在制订防止计算机或信息处理设备被滥用的法律，出于未经授权的目的而使用计算机有可能成为犯罪行为；要教育用户自觉意识到他们允许访问的范围是基本的安全要求；明确要求所有员工及第三方用户除非经过授权，否则对信息处理设备的任何形式的访问都是被禁止的。

应该在计算机屏幕上显示登录警告信息，指出进入系统是需要授权的，否则是不允许登录访问的。合法用户必须确认屏幕上提示信息的含义，计算机内的安全控制机制将限制未获得授权登录的响应信息，并制止其继续登录过程。

6. 使用密码技术的限制

国家通过法律、法规或其他措施加强对使用密码技术及其设施的管理。控制措施如下：

- 在我国设立国家密码管理局，对商用密码技术及其设备的开发、生产、销售和使用进行管理，管理的内容包括对从事密码技术研究、设备开发、生产、销售的企业实行经营资质和范围的审核、批准、年审制度，对商用密码的使用实行报批制度；
- 对于进口和出口具有加密功能的硬件和软件产品依法严格执行许可证制度；
- 在设计中包含加密功能的软件和硬件产品按规定申报，并在获批准之后才能生产和销售。

组织在决定信息系统中应用密码技术或设备保护信息机密性时，应该通过咨询确保遵守国家法律。在加密信息和加密设施转移或跨越到另一个国家之前，同样应该考虑遵从出入国的法律限制。

7. 证据收集的控制

1）证据的可用规则

收集证据对确定一个人或组织的操作行为的真实性及其责任是必要的，如果这种证据是用于在组织的内部追究责任人，那么证据的充分性应通过内部的操作规则予以描述。

一旦一个人或组织的操作行为涉及违反法律条款(无论是民法还是刑法),所提供的证据应该符合相关法律或者该案件受理法院规定的规则。一般来讲,这些规则包括:

- 证据的(真实)可信性,符合法庭采信规则;
- 证据的质量和完备性;
- 出具适当的证据,证明提供给法庭的证据的确在系统存储和处理期间被正确和一致地操作过。

2)证据的可信性

为了保证证据的可信性,组织应该确保用于采集证据的产品是依从已公布的采信证据产品的标准或操作规范的。

3)证据的质量和完备性

为了保证证据的质量和完备性,需要严格的证据跟踪。一般来讲,这种跟踪的严格性在下面的条件下成立。

- 对于纸质文档:原始版本文档应该被安全保管,并且对证据发现者、发现的地点、发现的时间以及证据发现过程的见证人予以记录,所有的调查都应该确保原始版本文档没有被篡改;
- 对于存储在计算机介质上的信息:应该将任何可移动介质(例如硬盘或者移动存储器)中的信息复制到固定存储设备,对复制过程中的所有操作活动的日志及介质上信息的复制品予以安全保管,确保其不被修改。

一个事件刚出现时,并不一定表明可能会引起诉讼活动,但应意识到事件可能继续扩大以致出现严重后果的可能性,这就存在事件演变过程中,必要证据遭受意外损坏或毁坏的风险。为此,建议大中型信息系统的管理机构对任何可能引起诉讼的事件(不论事件大小或引起诉讼的概率),在发现其苗头时,启动对证据的收集和保全的控制措施。

6.10.2 遵从安全策略和技术标准

信息系统安全保障的必要性和充分性应该定期检查,确保其符合组织的安全策略和国家或行业的技术标准。

执行检查时,应该遵从组织的安全策略;对信息系统的安全检查应该重点复核安全措施实施的技术标准,以及信息系统变更后的安全技术措施的必要性和充分性。

1. 遵从安全策略的检查

管理者应该确保责任范围内的所有安全规程得到正确实施。另外,对组织内的所有领域应该进行定期检查,以确保遵从安全策略。检查对象如下:

- 业务应用系统;
- 系统供应商;
- 信息和信息资产的所有人;
- 用户;
- 管理人员。

信息系统的所有人员都应该支持(包括协助、配合和接受)经常性检查。

2. 技术标准遵从性检查

应定期检查信息系统遵从安全技术标准的正当性和充分性。技术标准遵从性检查涉及

操作系统、数据库管理系统、业务应用系统、通信设施和运行环境的安全技术保护措施的合法性、有效性。这种类型的遵从性检查要求由技术和管理专家主导。

遵从性检查包括文档查阅、现场检查、座谈、调查以及渗透测试等。渗透测试可以邀请有资质的第三方机构或特聘专家独立进行。遵从性检查对于发现的脆弱性和验证安全技术控制措施的有效性是必要的。不过渗透性测试规程应该经过技术论证，小心演练，以免渗透测试危害到系统的安全性或意外地引入风险。

任何技术标准遵从性检查都只能由有能力的、经授权的专业人员进行。

6.10.3　系统审计方面的考虑

审计的任务是依照组织的安全策略对信息系统操作行为的合法性、合规性进行审查并提出改进意见，依照国家法律和安全技术规范对信息系统采取的安全措施的正当性、有效性和充分性进行审查，并提出处理意见。在对业务应用系统进行审计时，应制定周密的审计方案；应采取控制措施保护审计工具，以防止对审计工具的滥用和误用，避免对审计过程的干扰。

1. 对审计过程进行控制

应该仔细规划和协商审计需求，制定出审计方案。在涉及对操作系统等进行检查时，要避免中断业务流程的风险，为此应该遵守以下措施规范：

- 审计项应根据组织的安全策略制定，并得到信息系统所有者和管理者的同意；
- 对业务应用系统的审计一般应局限于对软件和数据的只读访问；
- 必要时，只对系统文件的复制件进行审计。在审计工作完成之后，审计人员应该和被审计的有关人员一起对其予以删除或销毁；
- 对审计所需的信息系统资源应该进行明确的标识，并在审计工作结束后保持其可用性；
- 当审计过程中涉及对特殊的或额外的信息资源进行处理时，应进行标识，并获得信息资源管理人的同意；
- 对审计活动进行过程监督，并全程记录，制成标准文档；
- 对审计过程所涉及的工作流程予以详细记录，连同审计责任人、被审计人的信息一起形成文档。

2. 对审计工具的保护

对审计工具软件的访问(如调用审计软件或读取审计数据)必须严格予以控制，以防止对审计工具软件的滥用、误用和对审计信息的修改。这些工具软件应在进行标识后，与开发工具和操作系统隔离保管，不应保留在磁带库或用户区内。如无法做到隔离，则应给予特别的保护控制措施。

6.11　习题与思考题

1. 信息系统在建设期间可能需要第三方参与，举例说明第三方参与可能带来的信息安全风险以及如何防范或控制这些风险？

2. 某组织的信息系统中有一些需要与其他组织共享的信息和处理设备，举例说明该组

织应对被共享的这部分信息系统资产进行哪些安全管理措施？

3. 某组织的信息系统将所有业务数据委托给电信服务商管理或放在云端服务器中，请问该组织在与电信服务商或云端服务商的合作中应考虑哪些安全风险以及如何防范和控制风险？

4. 对信息进行分类在信息安全管理中有哪些好处？举例说明在信息系统定级管理中如何使用信息分类技术。

5. 按员工聘用前、上岗、在岗、解聘 4 个阶段分别说明从信息安全管理角度应做哪些考核、审查、培训和监管工作？

6. 举例说明信息系统中安全区域、安全域和安全交接区在概念上的区别。

7. 从保护信息和信息处理设备的角度举例说明桌面清空和屏幕清屏的意义，以及应有怎样的操作行为习惯才能做到对信息和信息处理设备的安全保护。

APPENDIX A

附录 A 与本书有关的术语

access control(访问控制,存取控制)

限制与管理用户、程序、进程或计算机网络中其他系统访问被保护信息系统的资源的过程,这是管理和限制使用计算机系统或网络信息系统中资源的措施。一个组织或机构为保证网络信息系统内的信息资源免于未授权的访问,一般由系统管理员基于用户(也包括程序、进程或计算机网络中的其他系统等,下同)的标识符和它们在一些预先定义的用户组中的成员关系,采用软/硬件措施强制控制用户及用户的代理可访问的对象(如服务、目录、文件和数据流等),以及可进行的操作(如只读或可写)等。这种限制与管理活动称为访问控制,如果控制是明确地施加于存储系统中的数据,也可称为存取控制。

访问控制防止实体对资源的未授权使用,包括防止以未授权方式使用某一资源。这种服务对开放系统互连的信息系统中可访问资源的非授权使用提供限制能力。这些可访问资源可以是经开放系统互连协议访问的开放系统互连资源或非开放系统互连的资源。

为了判断一个实体的可访问权,访问控制机制可以使用该实体已鉴别的身份,或使用有关该实体的相关信息(例如它与一个已知的实体集的从属关系),或使用该实体的权力。如果这个实体试图使用非授权的资源,或者以不正当方式使用授权资源,那么访问控制功能将拒绝这一访问企图,并可能向系统管理员发出告警信息,或将其访问行为记录下来作为安全审计跟踪的线索。对于无连接数据传输,访问控制机制只能强加于发送者,当其发现发送者违反访问控制策略时,将拒绝原发的连接。

访问控制机制可以建立在下列一种或多种手段之上。

- 访问控制信息库:保存实体的访问权限,这些信息可以由授权中心保存或由正被访问的实体保存,这些信息的形式可以是一个访问控制表或者等级结构或分布式结构的矩阵,还要预先假定对实体的鉴别已得到保证;
- 鉴别信息:例如口令,对这一信息的占有和出示,证明正在进行访问的实体已被授权;

- 权力：对它的占有和出示证明有权访问由该权力所规定的实体或资源，权力应是不可伪造的，并以可信赖的方式进行传送；
- 安全标记：当与一个实体相关联时，安全标记可用来表示同意或拒绝访问，通常根据安全策略而定；
- 试图访问的时间；
- 试图访问的路由；
- 访问持续期。

访问控制机制可应用于通信联系中的一端点或应用于任一中间点，涉及原发点或任一中间点的访问控制是用来决定发送者是否被授权与指定的接收者进行通信，或是否被授权使用所要求的通信资源。

在无连接数据传输目的端上的对等级访问控制机制的要求在原发点必须事先知道，还必须记录在安全管理信息库(SMIB)中。

ACL(Access Control List，访问控制表或存取控制表)

信息系统中主体的所有访问权力的集合，或对受控对象的访问控制策略的集合，或与某对象相关联、标识了可访问该对象的所有主体及访问权力的一种列表。绝大多数业务应用系统的运行都允许对服务有选择地使用。访问控制表就是对服务进行控制的手段，由它来允许或拒绝访问。

active attack(主动攻击，积极攻击)

一类恶意的攻击。在这类攻击中，攻击者以各种方式(如中断、修改、删除、伪造、添加、重放、乱序、制造病毒等)破坏信息或系统。主动攻击的一个重要的特点是改变被攻击对象的状态，请比较 passive attack。

administrative security(管理安全)

为信息和信息系统资源提供适当等级的保护而建立的一些管理上的限制、操作过程、责任范围规定以及附加控制等。

application gateway(应用网关)

建立在网络应用层上、处于内部网络和外部网络的边界上的网关。这种应用网关设备不允许外部网络与内部网直接通信，沿途用一系列代理服务器过滤流入或流出网络的信息。用户可以把应用网关想象成一种安全代理，为内部和外部的两端代言，而不允许它们直接访问，从而达到隔离、保护目的。参见 Application-Level Firewall。

Application-Level Firewall(应用级防火墙)

由应用网关及有关代理服务软件构成的防火墙系统，又称双穴网关防火墙。在这种防火墙系统中，通过维持完整的 TCP 连接状态和进程提供所需的服务。应用级防火墙常常对通信进行重编址，以至于发送出去的分组看起来并不是从内部主机发出的，而是由防火墙发出的。参见 application gateway。

arbitrated digital signature(仲裁数字签名)

一类数字签名。根据接收者验证签名的方式可将数字签名分为真数字签名和仲裁数字签名两类。在采用仲裁数字签名方式时，签名者把签名消息经由被称为仲裁的可信的第三方发送给接收者，接收者不能直接验证签名，签名的合法性是通过仲裁者作为媒介来保证的。

asset(资产)

需要保护的信息或信息系统资源。资产是信息系统中对一个组织具有价值的任何东西和事物(包括硬件的或软件的,有形的或无形的,货币化的或非货币化的,等等),其中构成信息系统的资源要素是最直接的资产。

asymmetric cryptographic system(非对称密码体制)

含有两个相关变换的密码体制,一个是用公开密钥定义的所谓的公开变换,另一个是用私有密钥定义的所谓的秘密变换。非对称密码体制具有“根据公开变换来确定秘密变换在计算上是不可行的”特性。

asymmetric key(非对称密钥)

在非对称密码体制中,密钥成对出现,加密用的密钥和解密用的密钥不同,而且从其中一个密钥推导出另一个密钥在计算上是不可行的。

asymmetric key system(非对称密钥体制,非对称密钥系统)

一种密码体制或系统。它使用一个加密算法(或密钥)进行加密,而使用另一个解密算法(或密钥)进行解密。公开密钥密码体制是非对称密钥体制的一个用例:加密算法或密钥是公开的,解密算法或密钥是秘密的。

attack responses(攻击响应)

当在网上探测到攻击时,要求系统进行响应并立即采取行动。其响应形式取决于攻击形式、等级或相应的过滤准则;所有这些都取决于系统的安全策略和安全管理。例如,一般的安全系统(或安全管理工具)可提供以下形式的攻击响应:自动消除基于 TCP 连接的攻击,将攻击特征记录到数据库,通过电子邮件通报给安全管理器,重放攻击特征,以实时方式将攻击特征送到用户接口,等等。

audit(审计)

为检测整个系统的安全(特别是数据的机密性、完整性和可用性)的有效性和充分性而对设备、程序、活动和进程进行的检测和评估,以及对其中发生的通信或操作事件进行跟踪监视、分析与报告的过程。

audit trail(审计跟踪)

系统活动的流水记录。该记录按事件从始至终的路径、时间顺序重现、审查和检验每个事件或活动出现的环境及其合法性。

authentication(鉴别)

一种和身份有关的事务,用于确认一个实体所宣称的身份的过程。鉴别既应用于实体又应用于信息本身,如验证用户、设备和其他实体的身份的合法性或数据的完整性。鉴别通常被划分成实体鉴别和数据源鉴别两大类。例如,用户在登录进入一个多用户或网络系统时,鉴别处理系统将用户名和口令与授权的用户列表进行比较。如果匹配,则该用户为合法用户,并允许访问,其访问范围在许可列表中加以规定。对用户的这种检测过程称为用户鉴别。又如,在报文传输中,通过在报文中增加一个专门用于鉴别的字段,接收方可用已知的特殊编码对报文进行验证,以确定该报文在传输过程中是否被修改或遭到破坏,称为报文鉴别。

authorization(授权,授予权限)

授予用户、程序或进程对信息系统资源的访问权,包括允许基于访问权的访问。在

典型的情况下，权限由系统管理员设置，决定授予一个用户、程序或进程访问哪些计算机资源的资格或权力，而由系统按一定形式的鉴别标识符（如用户名和口令）进行鉴别和验证。

backup（备份）

构成信息系统的资源要素的替换品（例如复制品、冗余组器件），以及对信息系统运行的系统性数据或业务进程的动态数据的实时复制。当信息系统在出现故障不能或中断运行时，或系统组（器）件或数据丢失、损坏和不可用时，用来将信息系统或数据恢复到中断前的状态。这些备份在任何信息系统的运行环境中都是关键的安全措施之一。

backup and recovery（备份与恢复）

信息系统管理的一个策略。通过日常的数据和系统备份，在发生软件或硬件故障而导致信息系统（部分或整体）不可用时，该策略可以使用数据和系统的备份将信息系统或其组件还原到最初备份时的状态。

back door（后门，秘密通道）

绕过安全控制而获得对程序、进程或系统访问的方法。后门通常是程序员在开发阶段创建的，一般用于修改、调试或维护，或软件在线升级等。用于调试或维护目的的后门应该在程序正式发行前删除，或将其封闭的方法移交给用户，且不得泄露给第三方。如果后门被其他人知道，或在正式发行前没有删除，就会成为安全隐患。

bastion host（堡垒主机）

一个可以承受攻击的硬件系统，它安装于外来攻击者可进入被保护网络的通道上。堡垒机常常是防火墙功能的补充组成部分，或者是“外部”Web 服务器，或者是公共访问系统。一般来说，堡垒机都运行某种形式的通用操作系统（例如 Unix、VMS、Windows NT 等），而不是基于 ROM 的或坚固的操作系统。由于堡垒主机能坚固地抵御攻击，并作为“对外窗口”在防火墙之外（例如非军事区）使用，因此它常常成为系统的牺牲品。

CA（Certificate Authority，颁证机构或证书机构）

一个可靠和可信的权威机构。它发行安全证书并确保证书的可信性，或证明一个用户和它们的公开密钥的身份。在信息安全策略的语境中，证书机构是一个被委托的实体，可以生成含有一类或多类与安全相关数据的安全证书。

compromising emanations（泄漏发射）

一种无意的与数据有关的或载有敏感信息内容的电磁信号辐射。这种电磁波一旦被截获和分析，就可能将传输、加工或处理的信息泄露给未授权者。

configuration management（配置管理）

ISO（国际标准化组织）为了对 OSI（开放系统互连）网络进行管理而定义的 5 种网络管理模式之一。配置管理子系统负责配置网络的初始化参数，并检测和判断网络的状态。

control zone（控制区）

包括多个用于处理敏感信息的设备，并在有效的物理和技术的控制之下，以防止未授权的进入或泄漏的网络空间。

countermeasure（对抗[措施]）

任何减少系统脆弱性和威胁以降低系统风险的行为、设备、规程、技术或其他措施。对抗措施可在信息系统的任何层级采用，包括程序模块、设备、系统或设施/环境。

countermeasures and controls(对策和控制)

对策、控制和安全措施通常在安全领域作为同义词使用。对策和控制指使用规程和技术阻止安全事件的发生,检测正在发生或已经发生的事故,以及提供对安全事故做出反应或从中恢复的能力;安全措施可能是附加或增强用户的口令,对关键设备和数据的备份,能将具体的行为与操作人员关联起来的审计跟踪,或其他任何适当的技术或规程。

cryptanalysis(密码分析(学))

① 密码学中的一个分支学科,它和密码学的另一个分支学科——密码编码学是两个相互对立、相互依存、相辅相成、相互促进的学科。

② 它是企图挫败密码术(更一般地说是信息安全)的数学技术学科。在密码学中,它是对密码体制、密码体制的输入/输出关系进行分析,以便推断出机密性变量(包括明文在内的敏感数据)。

③ 在密码学中,在不知道加密算法所使用的密钥的情况下,将已被加密的消息转换成明文要做的步骤和操作称作密码分析,有时又称作密码破译(codebreaking)。

④ 密码分析依赖于自然语言的多余度,使用"分析——假设——推断——证实(或否定)"的四步作业方法,基本数学工具是统计分析、数学演绎和归纳。

cryptographic key(密钥)

密钥是一个秘密参数,或一组秘密参数,或一个秘密符号,或一个秘密符号序列。密钥用来控制加密/解密运算;密钥是密码体制(算法)中的可变因素;密钥仅被拥有它的人可知、可用。

cryptographic techniques(密码技术)

通常是指对信息(包括话音、数据和图像等)加以保护所用的密码编码/译码(加/解密)技术。一般将密码技术划分成两类,即对称密钥密码技术和非对称密钥密码技术。

cryptography(密码编码学,密码术)

① 密码编码学是密码学(cryptology)的一个分支学科,研究与信息安全(例如数据机密性、数据完整性、实体鉴别及数据源鉴别等)有关的数学技术学科。

② 密码编码学是包含数据变换的原理、方法和工具的一门学科,这种数据变换的目的是为了隐藏数据的信息内容,阻止对数据的篡改以及防止未经许可使用数据。

③ 密码编码学是论述使明文变成不可理解形式的艺术和技巧。

④ 密码编码学是密写的科学和研究科目。一种密码就是一种密写的方法,利用它可以把明文变换成密文。把明文变换成密文的过程称为加密;其逆过程,把密文变换成明文的过程称为解密;加密和解密都是用一个或多个密钥和算法来实现的。

cryptology(密码学)

密码学包含密码术和密码分析两个学科的领域。

data integrity(数据完整性)

信息系统中的数据和其原始数据相同,并未遭受未授权的偶然或恶意的生成、增加、删除、篡改、插入或破坏时所具有的一种特性。数据完整性有两个方面,即单个数据单元或字段的完整性以及数据单元流或字段流的完整性。一般来说,用来提供这两种类型完整性服务的机制是不相同的,尽管没有第一类完整性服务,第二类服务是无法提供的。

data protection(数据保护)

确保数据的机密性、完整性和可用性的过程。

data security(数据安全)

保护数据免受偶然的或恶意的创建、增加、删除、篡改、插入等破坏或泄露。

digital signature(数字签名)

一种基于加密和秘密授权代码的个人鉴别方法,等效于手写签名,用于“签署”电子文档。数字签名实际上是一个把数字形式的消息和某个始发实体相联系的数据串,把它附加在一个消息或完全加密的消息上,以便于消息的接收方能够鉴别消息的内容,并证明消息只能始发于所声称的发送方。

disaster(灾害,灾难)

任何使一个组织或机构不能进行其关键业务活动的事件。相似的术语有 business interruption、outage、catastrophe 等。

disaster plan(灾难(应急)计划)

作为信息安全策略的一部分,灾难应急计划规定了信息系统遭遇灾难事件或服务中断后的紧急反应、备份操作和恢复等活动规则,以达到恢复系统正常运行的目的。

DMZ(De-Militarized Zone,非军事区)

一般指处于军事对抗双方之间的缓冲区,这里指一段不安全的 LAN(局域网)或 WAN(广域网)区域。通过这个网段将被保护网络与外部不可信网络隔离开来,形成对抗之间的缓冲区。通过安装防火墙,被保护网络可以容忍 DMZ,或与它们相连接。

encipherment(加密,译成密码)

对数据进行密码变换产生密文的过程。加密既能为数据提供机密性,也能为通信业务流信息提供机密性,并且可以成为其他安全机制的一部分或起补充作用。

加密算法可以是可逆的,也可以是不可逆的,可逆加密算法有下面两大类。

① 对称(即加/解密使用相同的秘密密钥)加密:对于这种加密,知道了加密密钥也就意味着知道了解密密钥,反之亦然;

② 非对称(即加密和解密使用不同的秘密密钥和公开密钥)加密:对于这种加密,知道了加密密钥并不意味着也知道解密密钥,反之亦然,这种系统的这样两个不同的密钥有时称为“公钥”与“私钥”。

Encrypt(加密)

用一个密码体制把明文变成不可理解形式,变换的结果称作密文。

Ethics(道德规范)

依靠信念、教育、社会舆论和传统习惯等约束条件对人与人和人与社会之间的关系进行规范和自我行为调整的准则的集合。它是个人或社会活动经验的产物,是一个基础性的为大多数人所公认的共识,在做决定时用来判断对与错。遗憾的是,在当今开放互连网络环境下,道德规范却因环境变化发生错位。例如,某些人可能认为闯入别人的房间是错误的,但却不认为闯入别人的计算机系统内部是错误的。

entity authentication(实体鉴别)

确认要求被鉴别实体就是其所声称的实体的过程。

event(事件)

在网络信息系统中出现的对其信息和系统构成要件的非常规操作或未预期的重大情况。

event testing(事件检测)

与安全有关的事件检测包括对安全事件的检测，也可以包括对“正常”事件的检测，例如一次成功的登录(或注册)或登录失败。对与安全有关的事件的检测可由 OSI 内部含有的安全机制来做，也可由监控与审计工具来做，构成一个事件的技术规范由事件处置管理程序来维护。对各种安全事件的检测可能引起下列一个或多个动作：

- 在本地报告这一事件；
- 远程报告这一事件；
- 对事件作记录；
- 进行恢复。

这种安全事件的例子如下：

- 特定的安全侵害；
- 选择的特定事件；
- 对事件发生次数计数的溢出(超出预定数值)。

事件检测的技术规范需要考虑对事件报告与事件记录的格式，以及为了传输事件报告与事件记录所使用的语法和语义的定义。

evidence(证据)

用于解决纠纷与确定责任的信息体或数据集合，或与其他数据链接用于解决纠纷与确定责任的数据(集合)。

failover(故障自动备份)

在集群网络系统(有两台或多台服务器互连的网络)中自动将出现故障的资源或服务转移到备用的资源或由备份系统继续提供服务的过程。出故障时，自动备份功能将在检测到服务器、网络适配器、磁盘驱动器和其他设备上的任何故障后，自动切换到备用部件上，以保证为用户提供不间断的服务。

failure control(故障控制)

在信息系统中用于查出硬件和软件故障，并提供故障恢复或故障弱化的方法。

failure management(故障管理)

由 ISO(国际标准化组织)为 OSI(开放式系统互连)网络的管理所定义的 5 种网络管理模式之一。故障管理试图确保网络故障被检测出来，并将其控制。

failure tolerance(容错)

在发生诸如电源不足或硬件故障等灾难性事件或故障时，计算机或操作系统能够确保不丢失数据，并且当前运行状态不会受到破坏的一种处置能力。它可以通过配置诸如后备电源、备用硬件和软件等方法实现。在容错网络中，系统可以不丢失数据而继续运行，也可以关机后重新启动，并在重新启动时，恢复故障发生时正在运行的所有处理进程。

filter(过滤，过滤器)

在网络中按照信息流或数据包的某些特征(如源地址、目的地址或协议等)或模式对网络信息流进行筛选，并且根据已建立的准则确定是否转发或放弃该信息流，这种处理过程称

为过滤。完成过滤任务的可以是一种设备，也可以是一个程序，或程序的一组特性，或一种模式或掩码，称为过滤器。例如，一个电子邮件过滤器可以使用户滤除来自某些站点的电子邮件。

firewall（防火墙）

防火墙以逻辑隔离方式保护内部网络的安全，不严格地说，防火墙指拒绝未授权的外部用户访问内部特定主机或服务，或者未授权的内部用户访问外部网络的任何设备和方法。稍严格地说，指强加于两个网络之间的边界处，保护内部网络免遭来自外部网络的威胁，或控制内部用户未经许可对外连接的系统或系统组合。例如，配置了过滤功能的路由器或访问服务器，或几个这样的路由器或访问服务器，专门用作内网与外网之间的隔离或缓冲。这种系统或系统组合实际上是对内、外网络之间的通信进行监控的系统，其采用的主要技术包括数据包过滤、应用网关和代理服务器等。

防火墙有许多种类，一般可以分为两大类，即网络层级和应用层级的防火墙。网络层级的防火墙拦截所有尝试进出网络的报文包，扫描它的地址标识以确认连接源地或宿地，并按照安全策略规则予以判断，决定转发还是拒绝转发这个报文包；应用层级的防火墙由一个和网络隔离的计算机设备担任，由它执行各种应用服务的代理。当防火墙外的计算机提出要求连线服务时，代理服务器（proxy server）会主动按过滤规则执行这项要求。对于要求对内连接的计算机而言，无法和防火墙内的计算机直接相连，防火墙只是一个具有判断能力的转接设备。

由于防火墙的作用实际上是将被保护的网络对外屏蔽，因而不能防范来自被保护网络内部的安全威胁。

Firewalls and Separation of Duties（防火墙和职责分离）

防火墙和职责分离本是两个不同的概念，但却具有相似的功能结构和功能互补性：防火墙是一种隔离技术措施，它提供访问活动、系统或系统部件之间的隔离，以便限制不期望的访问或将系统缺陷对外隐蔽起来，且对其他访问活动或系统不产生影响（例如将局域网与因特网隔离，并不影响局域网内部的系统）；职责分离则提供系统内各个职能之间的隔离，其目的是保证没有一个独立的操作实体（通过单独行动）可以穿透整个应用系统，但这种隔离并不影响各自负责的那部分系统的操作能力。

恰恰是这两个不同的概念共同用在安全控制中，一方面作为技术上的隔离措施加强了基础安全策略，另一方面通过操作职能的分离控制对系统高风险的操作活动，避免单个操作实体穿透整个应用系统的事件。

flood（泛滥，淹没，充斥）

充斥或占满信息系统端口、缓存区及内存区等信息系统资源，例如使 TCP/IP 系统连接队列溢出，从而导致系统拒绝正常服务。

gateway of application layer（应用层网关）

能在应用层上实现协议转换或作为应用程序代理的网关。

Goals（（安全）目标）

信息系统的安全目标与系统所属组织的安全目标是完全一致的。信息系统的安全目标集中体现为两大指标，即信息保护和系统保护。

① 信息保护：保护所属组织的有价值信息和维系与系统运行有关的信息的机密性、完

整性、可用性和可控性。

② 系统保护：保护所属组织的运行和职能实现的技术系统的可靠性、完整性和可用性。

信息系统最低安全目标的确定基于信息系统运行的可靠性、完整性、可用性，信息数据的机密性、完整性、可用性和可控性，取决于各种安全威胁实施后的社会、政治和经济风险的大小，而社会、政治、经济风险的大小与信息系统所属的组织属性、社会功能/职能，以及所拥有的信息的敏感度和社会影响面的大小直接相关。

group account(组账号)

一组用户共同使用的账号。给一组用户分配一个用户账号，使该组全体成员拥有相同的权力和许可。

group digital signature(群数字签名)

由 Chuam 和 Van Heijst 提出的一种数字签名方案，它允许群中的各个成员以群的名义匿名地签发消息。群数字签名的特点如下：

① 只有群的成员才能代表那个群签发消息。

② 签名的接收者能验证它是那个群的一个合法签名，但不能揭示它是群中的哪一个成员产生的。

③ 在后来发生争端的情况下，借助于群成员或一个可信的机构能识别出群里的那个签名者。一个群数字签名主要由签名算法、验证算法和识别算法 3 个算法组成。这种签名的一个实用的例子是投标，在这里，成员是每个提交投标的公司，群是所有提交投标的公司。

Hackers/Crackers(黑客/骇客)

中文黑客为 hacker 的音译，取意 hacker 则指那些喜欢留下痕迹的人，后被美国舆论界用来特指那些对计算机技术、计算机编程和因特网特别感兴趣，且有较高专业知识和相当操作技能，热衷于程序设计和计算机新奇应用的人。这些人喜欢检查操作系统和其他程序的源代码，以弄明白它们是如何运行的。他们通过运用高超的编程技巧使计算机的性能发挥到尽可能的程度。后来，此词被转义用来指那些利用计算机系统的安全脆弱性和设计缺陷直接或绕过控制进入、阻挠、窥视他人计算机系统的计算机编程高手。黑客凭借自己掌握的计算机技术专门刺探信息系统中存在的安全漏洞，非授权地访问计算机网络，窥视别人在计算机网络上的秘密，阻止信息系统的正常运行，搞恶作剧式的数据破坏，甚至进行更严重的计算机犯罪。多数黑客的目的仅仅是为了炫耀自己的技能或恶作剧。政府、军队、企业、大学和研究机构的机密性资料都在他们的窥视之列，有的黑客甚至刺探个人隐私。黑客中有的人截取银行账号，盗取巨额资金；有的盗用通信号码，使电信公司和客户蒙受巨大损失；有的黑客在搜索到企业的重要秘密后，甚至可能对企业采取绑架式威胁，以获取非法利益。此类黑客的存在对计算机系统的安全与保密构成极大威胁。但是，也有一些过去的黑客“改邪归正”，归正后有的甚至成为计算机安全系统的专业设计人员(当然，对是否雇用从前是黑客的人做安全人员，业界有分歧)。

总之，黑客作为一个群体不应简单地用某一个或某几个具体属性去定义。但是，从建立信息系统的有效秩序和维护社会秩序来看，不接受管理和不受法律约束的黑客行为是不能容忍的。

在因特网术语中，一般认为黑客不是贬义词。那些专门从事不良行为的人不是一般意

义上的黑客，而被称为 Cracker（骇客）。

heterogeneous network（异构网络）

由不同厂商生产的网络设备组成的网络，这些网络设备运行不同的协议，并且在很多情况下支持不相似的功能或应用，不同厂商的设备的协议不兼容。

homogeneous network（同构网络）

早期由网络厂商按自己的网络交换协议设计的单一结构的网络，这种网络内的所有网络设备只运行该厂商提出的网络交换协议，不同的网络之间不兼容。

I&A（Identification & Authentication，标识与鉴别）

主体是其身份可被鉴别的实体。标识将可辨别标识符（identifier）与某一主体联系起来，以与其他主体加以区别。一个主体可以拥有或使用一个或多个用于将自身与其他主体相区别的辨别标识符。鉴别是利用实体的标识符验证主体所宣称的身份的过程，得到这类验证的主体身份称为已鉴别身份。

ID（IDentifier，标识符）

用作标识的唯一的文本字符串，机器通过它可以读出识别信息，然后由系统对实体进行鉴别。

identification（（身份）识别）

指定的用户向系统出示身份证明的过程。这是为防止假冒攻击采用的一种技术，使得一个用户能获得另一个用户（申请者）身份的确是其声称的身份的保证。其最常用的技术是由一个验证者检验一个消息的正确性，从而说明申请者拥有一个与其真实身份有关的秘密。

information system（信息系统）

① 一种系统，由为了收集、处理、传输和存储表达用户信息的数据而组织起来的人、机器和方法组成，而不管它是自动的或手动的。

② 任何远程通信和与计算机有关的仪器或互连系统，用于获取、存储、操纵、管理、移动、控制、显示、交换、转换、传输或接收音频、图形、图像视频和数据，并且包含软件、带有微程序的固件和硬件。

③ 在开放互连的网络环境下，指用于信息收集、处理、存储、发送、显示、传输和交换的整个通信基础设施，以及组织、人员、数据、通信协议、应用程序和运行环境的总和。

INFOSEC（Information System Security，信息系统安全（体系））

确保以电磁信号为主要形式的，在计算机网络系统中进行获取、处理、存储、传输和利用的信息内容，在各个物理位置、逻辑区域、存储和传输介质中，处于动态和静态过程中的机密性、完整性、可用性、可审查性和抗抵赖性的，与人、网络、环境有关的技术和管理保障措施的总和。这里的人指信息系统的主体，包括各类用户、支持人员以及技术管理和行政管理人员；网络则指以计算机、网络互连设备、传输介质及其操作系统、通信协议和应用程序所构成的物理的和逻辑的完整体系；环境则是系统稳定和可靠运行所需要的保障系统，包括建筑物、机房、动力保障与备份以及应急响应与恢复系统。

从系统过程与控制角度来看，信息系统安全就是信息在存取、处理、集散和传输中保持其机密性、完整性、可用性、可审计性和抗抵赖性的系统辨识、控制的策略和过程。

integrity（完整性）

一种提供开放系统互连保护的服务，它防止信息系统的信息或资源被未经授权进行新

建、插入、篡改、增加或删除等。数据完整性保护是完整性保护的具体实例。参见 data integrity。

Internet(因特网,国际互联网,网际)

"Internet"(注意大写"I")是世界上最大的互联网。因特网由 ARPANET 的一部分演化而来,有一段时间被称为 DARPA 互联网或 ARPA 网络,它是用 TCP/IP 协议族连接的国际间的互联网,由美国的 MILNET、NSFnet 和 CREN 等网络以及遍布全球的无数区域网和园区网组成。由于使用统一的 TCP/IP 协议族,使它们成为标准统一的、协调的网络。因特网是网络和网关的大集合。在物理上是由一些网关和协议把多个报文分组交换网互相连接起来的一个集合。这个集合使得这些网络在逻辑功能上形成一个单一的、大型的虚拟网络。因特网提供了通用连接性和三层网络服务,即不可靠的非连接报文分组投递、可靠的全双工式数据流投递,以及建立在这两种服务上的应用层服务,例如电子邮件。因特网最早联通了美国的许多大学、研究实验室和政府机构,是一个三级分层,由中枢网络(即 Ultranet)、中级网络(即 NEARnet)和存根网络组成。现在这个术语用来表示采用 TCP/IP 协议族的全球互联网,它与全世界各种局域网络互连互通,并且形成了以实际生活应用为基础的研究和标准化的"文化"。很多前沿网络技术都来源于因特网社团。注意,不要把 Internet 与一般术语 internet 相混淆。

internet(互联网)

internet(注意小写"i")是 internetwork 的缩写,强调的是使用互连技术连接的网络,不要与 Internet 相混淆。

intrusion detection(入侵检测)

入侵检测是一种对入侵信息系统的行为进行检测的技术,其目的是检测和识别对系统的入侵与攻击行为,以便及时发现正在非授权进入受保护系统的入侵者。入侵检测范围包括误用、入侵或非法行为。常见的入侵检测技术有两种类型,一种是异常检查,它通过对流量统计的偏差检测出不正常的行为或安全策略的缺陷;另一种是模式匹配,它将用户活动和一系列已知的入侵与攻击行为特征进行比对分析,从而发现入侵和攻击行为。

key(密钥)

在密码术中,密钥是一系列控制加密、解密操作的参数或符号。参见 cryptographic key。

keys to incident prevention(防范事件的关键要素)

一些信息安全事件是可以避免的,条件是信息系统中的相关人员在他们的日常工作中牢记下面 3 个基本要素:

① 安全意识,个人应该意识到他们用于作业的资产的价值以及与此对应的威胁和脆弱性的本质;

② 个人必须坚持与维护已建立的安全措施(例如磁盘扫描、改变口令、实施备份等);

③ 在操作中遵守规程,小心谨慎。

LAN(Local Area Network,局域网)

一种覆盖一个相对较小物理区域的高速、低错率的数据网络。这里的高速率通常为每秒几十兆位到每秒几千兆位;覆盖面积较小,指跨度一般为几十至几千米。LAN 把工作站、外围设备、终端和其他网络设备连接在一个建筑物内或其他有限的地理区域内。高速是

因为这个网络只覆盖一个小区域,网络中的信号通信协议可以被优化。LAN 的技术标准规定了在 OSI 模型的物理层的电气规范和数据链路层中的信号分帧及传输方式。以太网、FDDI(光纤分布式数据接口)和令牌环(Token Ring)等是广泛应用的 LAN 技术。请比较 MAN 和 WAN。

laws and Regulations(法律法规)

建立基本控制/安全目标必须遵循的法制性规范的集合。

least privilege(最小特权,最低特权)

① 在设计操作系统时,以保留最小系统特权为准则,这样可限制授权的级别,获得授权只允许进行有限操作,从而减少具有高级特权的进程或用户执行授权操作而引发安全问题的机会。它要求系统赋予操作主体的授权必须遵循最小特权限制的原则。这一原则的应用可限制事故、错误、未授权使用带来的损害。

② 在信息系统安全中,任何实体(用户、管理员、进程、应用和系统等)仅有该主体需要完成其被指定任务所必需的特权,从而可以尽量避免将信息系统资源暴露在侵袭之下的可能,并减少被侵袭所造成的破坏。

logging(日志(记录))

在信息系统中指对发生在系统处理设备和安全保护设备运行中的操作或通信事件过程的流水记录。例如,记录发生在防火墙或网络设备上的有关事件的流水过程。日志基本上是按事件发生的时间顺序记录的,当累积到一定阶段时再予以分类整理。

MAN(Metropolitan Area Network,城域网)

一种用来服务一个近似于大城市区域的数据网。城域网是在一个城市范围内运行的网络,或者在物理上使用城市基础电信设施的网络,其规模小于广域网,但大于局域网。这种网络以更高速度(通常为每秒几百兆位到每秒几千兆位)并足以覆盖整个城市地域的规范运行。请比较 LAN 和 WAN。

media(介质,媒体)

medium 的复数形式,进行数据保存和信号传输的各种物理空间。常见的电子数据存储介质有各种存储器件、磁带、光盘、软盘和硬盘存储装置(固定的和便携式的),常见的网络传输介质有双绞线、同轴电缆、光纤电缆和大气(通过它进行微波、激光和红外传输)。它有时也叫物理介质(physical media)。

Need to Know(应知)

在信息系统中为培训和学习操作规程而制订的理论知识和方法的基本要求集,涉及两个方面:首先,完成操作所需访问的信息及访问规程;第二,为适应操作的变更需要继续学习的东西。在第一种情况下,对信息和进程的访问仅限于要求完成操作的个人。这种方法将未授权活动的可能性最小化,这就要求个人对与信息系统的使用或维护相关联的威胁和脆弱性的本质进行最大程度的理解。在第二种情况下,要求个人对快速发展的信息技术特征有必要的了解,以便更好地认识其中的脆弱性。

network encryption(网络加密)

在网络通信安全中,通过网络传输加密消息的技术,涉及网络通信加密的方法有 3 种,即链路加密、结点加密和端端加密。

链路加密要求对不同通信链路配置密码设备,因此消息在进入通信链路之前被加密,在

离开该链路之后解密，再在进入下一通信链路之前用一个不同的密钥将信息加密，如此重复直至到达信息传输的接收地；结点加密则是先为进入结点的加密消息提供解密，并为传输到下一结点用一个不同的密钥再将信息加密；端端加密不涉及中间结点的解密和再加密，一般在网络层的信息传输的两端进行加/解密操作，目前最常见的是在 IP 层采用 IPSEC 协议进行的加密，这样只需在通信路径两端配置密码设备即可。

network-Level Firewall（网络级防火墙）

一种适用于网络层的防火墙。这种防火墙通常部署在被保护网络与外部网络的连接通道上，对出入被保护网络的信息流在网络协议分组一级进行检测和控制。

non-repudiation（抗抵赖，不可否认，不可抵赖）

用于防止发送者否认自己已发送过数据或其数据内容，以及接收者否认已收到过数据或其数据内容的特性。当由于一个实体不承认其一些行为或行为内容而发生争论时，解决这种纠纷就需要一种方法，涉及可信第三方的证明过程可解决上述争论。使用公开密码体制的数字签名的不可否认特性可以防止一个签名者签署一个文件，随后又否认其签名的行为。

NTP（Network Time Protocol，网络时间协议）

参照无线电和因特网上的原子钟以保证维持精确的本地时间的一种协议，这是一个在因特网上保证本地时钟准确计时的网络协议，它能使分布于各处的时钟在较长的时间段内保持毫秒级的同步。

packet（（数据）包，报文分组，分组）

通过报文分组交换网络进行发送的数据单位，它是计算机网络中传输数据时所用的一种数据包装形式。“packet”这一术语的使用是不严格的，在报文分组交换网络中使用报文分组进行传输，但在有些文献中此术语专指在物理网络中传输数据的单位，另外一些文献将因特网看作是一种报文分组交换网络，并将 IP 数据报描述为报文分组。

数据包是数据的逻辑组合，它包括一个含有控制信息的报头和用户数据，报头中含有报源地址、报宿地址及其他信息。用户要传输的数据可能很长，网络无法一次传输出去，于是把它分成许多较小的部分，并依次传送。为了重组原数据，每个部分都包含与原来相同的报头和对应的位置序号，这就是报文分组（简称包）。包常被用来表示网络层的数据组单元。术语 datagram（数据报）、frame（帧）、message（报文）与 segment（分段）也被用于描述在 OSI 参考模型的不同层与各种技术领域中的逻辑数据组。

packet filter（（数据）包过滤，包筛选，报文分组过滤）

报文分组过滤的机制允许授权的程序去影响帧的多路分用。应用程序使用包过滤器原语建立捕获报文分组的判据（如应用程序规定希望捕获在帧中的 type 段中的给定值的所有报文分组）。一旦操作系统接受了过滤器命令，它就开始把规定类型匹配的所有报文分组放到一个队列中。应用程序使用另外一部分报文过滤器机制从这个队列提取报文分组。报文分组过滤可以存在于路由器、网桥或独立的主机中，有时也称为分组屏蔽。它是在网络层上运行的技术，对网络层以上的信息则无理解能力，因此该技术本身对网络的保护功能是一些由系统提供的有限的专门机制，只允许应用程序与较低层的协议相互作用，所以在安全要求较高的场合，这种机制还必须配合其他技术来加强过滤。

passive attack(被动攻击)

① 在这类攻击中,攻击者以各种方式窃取信息,但不破坏信息(如修改、删除、伪造、添加、重放、乱序和制造病毒等)。被动攻击只威胁数据的机密性。

② 在密码技术中指一个密码破译方企图通过简单地记录数据和其后对这些数据的分析(例如在密钥编码中确定会话密钥)来挫败一种密码技术。被动攻击只威胁数据的机密性。请比较 active attack。

password(口令,通行字)

用来鉴别实体身份的受保护的或秘密的字符串,通常是用户访问分时系统或网络资源时输入的验证身份的代码。用户输入口令时,屏幕上并不显示所输入的字符,常常是显示一串相同的类似"*"这样的符号。不过,访问匿名网络服务虽然也要求用户输入口令,但所输入的口令可以是任意一串字符,例如"guest"。在网络应用中,有人将口令或通行字叫作密码,这在概念上是不严谨的,但这样说的人多了也就约定俗成了,我国银联 ATM 机最为普遍地采用了这一叫法。

physical security(物理安全)

应用物理障碍或控制规程作为应对资源和敏感信息风险的防护手段和对抗措施。

PIN(Personal Identfication Number,个人身份识别号)

访问控制中识别个人身份的标识号,在使用终端或访问、传输信息前,用户必须输入的唯一的个人号码。这个号码在有的场合也叫口令或通行字。

Ping Flooding(ping 泛滥,ping 淹没)

ping 泛滥是企图用报文包来阻塞或淹没网络通信连接的端口,以便减慢或阻止通过网络的合法通信流量。对网络目标主机进行一系列连续的 ICMP 回应请求(Echo Request)报文就会引起目标主机的 ICMP 回应(Echo Reply);连续的请求与回答报文将大量占用网络带宽,使网络变慢,引起合法通信流量的速度明显减慢,到最后完全堵塞。此类攻击能有效地破坏网络的连通性和可用性,所有 TCP/IP 系统均可能受到这种攻击。如果系统受到该类攻击必须找出 ping 源,然后使它停下来。当然,最好的办法可能是重新配置组织的外界路由器或防火墙,不允许 ICMP 请求到达组织的内部网络。然而,这并不能阻止由内部发起的 ping 泛滥攻击。

PKC(Public Key Cryptography,公开密钥密码学)

公开密钥密码学的思想是在 1976 年由迪菲和海尔曼(Diffie-Hellman)提出的。其基本思想是密钥成对出现,一个为加密密钥,一个为解密密钥,而且从其中一个推算出另一个是计算上不可行的。在这种密码体制中,加密密钥和算法公布于众,任何人都可用别人的加密密钥来加密自己要传送的明文消息。但是,只有拥有秘密的解密密钥的人才能将传送过来的已加密的明文(即密文)消息解密而得到原消息。

公开密钥密码体制又称作双密钥密码体制或非对称密码体制。

PKI(Public Key Infrastructure,公钥基础设施)

PKI 是一套集生成密钥、签发证书、分发证书、维护证书等功能于一体的公钥管理基础设施。其职能包括为用户生成密钥(公钥、私钥)、分发数字证书、管理数字证书、公布有效数字证书和无效数字证书等。PKI 本身不是具体的设施名称,属于 PKI 范畴的最基本的设施为 CA,即证书机构,此外还有 KMI(密钥管理基础设施)、PMI(权限管理基础设施)。

Policies and Procedures(策略和规程)

完成某一目标的方法和途径,以及实现这一目标的符合逻辑的规则和指令集。

privacy(个人保密权,个人隐私权)

不允许访问未经授权的账号或其拥有的数据信息的一种权力,它控制和影响与个体有关的哪些信息可以被收集、存储以及哪些信息可以被谁泄露和泄露给谁。由于这一术语涉及私人权力,其概念不可能精确地予以限定。

Quality Assurance/Quality Control(质量保证/质量控制)

在信息系统安全中指保证过程一致性和完整性等的一系列规范和措施。

redundancy(冗余)

信息系统中设备、服务或连接等的重复配置或部署,以便在故障事件后冗余的设备能接替执行那些故障部分应完成的工作。实际上,冗余是备份的一部分。

risk(风险)

① 在信息安全中,风险是由于威胁针对系统脆弱性进行开发和利用,从而给信息系统造成损失的潜在危险的总和。

② 在系统工程中,风险是对获取一个目标或与技术性能、价值、进度有关的需求时的不确定性的度量。风险级别按发生的概率和发生的后果来分类。风险的来源包括技术(例如可行性、可操作性、可生产性、可测试性和系统有效性)、开销(例如预算)、进度(例如技术/材料的可获性、技术成就以及重大事件),以及规划(例如资源、契约)等方面的因素。

risk analysis(风险分析)

在信息安全中指确定风险的时间空间分布及其等级,以此导出防范风险的安全需求的过程。风险分析是风险管理的主要组成部分。

Risk Management(风险管理)

确定、控制、消除或缩减影响系统资源安全属性和不间断服务能力的不确定事件的总过程,包括风险分析、费效分析、安全措施选择、实现与测试、安全防护符合度评估及所有的安全检查,其目标是将风险降低到能够获得和维持指定管理机构的批准。

因此风险管理可以理解为这样的一个过程,即将脆弱性、威胁和来自安全事件的潜在影响与实施安全措施的成本进行综合平衡。风险管理的目的是保证所有的信息资产得到正当的、充分的保护,避免不必要的管理资源开销。随着潜在威胁范围增大或可用资源减少,风险管理的重要性愈显突出。

router(路由器,路由选择器)

广义地说,路由器是负责决定在网络(特别是因特网)通信的多条通路中选择一条路径传送信息流的设备。在最低层,一个物理网桥就是一个路由选择器,因为它决定是否将报文分组从一条物理线路传送到另一条物理线路。在远程网络中,每个单独的报文分组单独选择路由。在因特网中,每个 IP 网关就是一个路由选择器,因为它使用 IP 报宿地址选择路由。路由器使用一个或多个准则来确定一个网络信息被转发的最佳线路,根据网络层信息和路由选择表做出传送决定。路由选择表的结构通常取决于路由选择协议。

狭义地说,路由器是工作于网络层的设备,位于网桥或 L2 交换机工作的 MAC 层之上。路由器使用网络层的信息来做出转发和过滤决定。第三层交换机和路由器之间的差别已经

变得很模糊,因为它们都是根据网络层数据做出判决。

路由器有时也称为网关(虽然这种网关定义正变得越来越不经常使用)。

security administrator (安全管理员(器))

在组织的信息系统中对于定义或实施安全策略的某一部分或多个部分负有责任的人或系统。

security audit(安全审计)

为了测试信息系统的安全控制措施或设备的性能是否足够,为了保证与已建立的策略和操作(过程)规程相符合,为了发现安全漏洞,以及为了建议在控制、策略和过程方面进行指定的改变,而对系统日志与活动进行的独立审查和分析。

安全审计提供了一种不可忽视的安全机制,它的潜在价值在于经事后的安全审计得以检测和调查安全漏洞,目的是测试系统的安全控制措施是否恰当,保证与既定策略和操作(过程)规程的协调一致,有助于做出损害评估,以及对控制、策略与规程方面指定的改变做出评价。安全审计要求在安全审计跟踪中记录有关安全的信息,分析和报告从安全审计跟踪中得来的信息。

收集审计跟踪的信息,列举被记录的安全事件的类别(例如对安全要求的明显违反或成功操作的完成),能适应各种不同的需要。已知安全审计的存在可对某些潜在的侵犯安全的攻击源起到威慑作用。

OSI 安全审计跟踪将考虑选择记录什么信息,在什么条件下记录信息,以及为了交换安全审计跟踪信息所采用的语法和语义定义。

security domain(安全域)

一个信息系统构成元素的集合,处于一个安全策略和一个安全机构管理下的物理或逻辑区域,其中,元素集合的特定行为服从安全策略,而该安全策略受到该安全域安全机构的管理。安全域的行为可涉及一个或多个不属于该域的元素,但至少有一个元素必须在域中。

security authority(安全机构)

在信息系统中对安全策略的定义、实现或实施负责的一个实体。

security domain authority(安全域机构)

在一个安全域内对实施安全策略负责的安全机构。

security label(安全标记,安全标签)

与某一信息系统资源(可以是数据单元、设备或进程等)密切相关的标记,这些标记为该资源命名或指定某些安全属性。这种标记可以是显式的,也可以是隐含的;可以是与资源分离的,也可以是与资源不可分离的。

包含数据项的资源可能具有与这些数据相关联的安全标记,例如指明数据敏感性级别的标记。常常必须在传送中与数据一起传送适当的安全标记。安全标记可能是与被传送的数据相连的附加数据,也可能是隐含的信息,例如使用一个特定密钥加密数据所隐含的信息,或由该数据的上下文所隐含的信息,又例如数据来源或路由来源隐含。明显的安全标记必须是清晰、可辨认的,以便对它们做适当的验证。此外,它们还必须安全、可靠地依附于与之关联的数据。

security policy (安全策略,安全政策)

为实现安全目标提供安全服务的一套准则,它是规定一个机构管理、保护与分发信息系

统资产的法规与条例的集合。

security requirements(安全需求)

为使设备、信息、应用及设施符合安全目标的要求，根据风险分析结果确定需要保护的对象、保护类型及保护等级。

security threat(安全威胁)

对信息系统进行潜在攻击的技术和方法。安全威胁可以划分为 3 个级别，其中 A 级威胁为信息战式的战争威胁；B 级威胁为有组织的分布式协同攻击；C 级威胁为个体式的信息攻击。安全威胁从行为特征上可分为 4 类，即主动威胁、被动威胁、偶然性威胁和故意性威胁。

security training(安全培训)

对安全应知应会知识进行灌输和训练。安全培训将信息系统涉及的与信息安全相关的知识传授给那些使用、维护或管理信息系统的人。经过良好培训的员工通过对信息系统进行精心的操作和维护，弥补安全控制措施和过程管理方面的不足或缺陷，提高安全保护技术和安全设备的保护效能。安全培训已被证明可以使信息安全措施的投资得到最大收益。

sensitive information(敏感信息)

由于有意或无意地泄露、修改或破坏可能造成损失或危害，因而需要某种等级保护的信息。

signature(签名，签字)

签名机制包括两个过程，即对数据单元签名和验证签过名的数据单元。

第一个过程使用签名者私有的(即独有的和机密的)信息，涉及使用签名者的私有信息作为私钥，或对数据单元进行加密，或产生出该数据单元的一个密码校验值。第二个过程所用的规程与信息是公之于众的，但不能够从它们推断出该签名者的私有信息，涉及使用公开的规程与信息来判定该签名是不是用签名者的私有信息产生的。

签名机制的本质特征为该签名只有使用签名者的私有信息才能产生出来，因而，当该签名得到验证后，它能在事后的任何时候向第三方(例如法庭或仲裁人)证明只有该私有信息的唯一拥有者才能产生这个签名。见 digital signature。

Social Engineering(社交工程，社会工程)

一种利用社会关系或社会交往间接地获取信息系统脆弱性或进入系统的方法，然后伪装目的地用户或管理员身份对系统进行攻击的技术或方法论。利用社会工程方法进行攻击的典型例子如电话用户或操作员自称是已获得授权的用户，然后试图获得对系统的非法访问。

switch(交换(机))

适用于电子或机械通信设备的一种通用术语。网络通信交换操作在 OSI 模型的数据链路层或网络层上进行。这些设备允许在需要时建立连接，并在连接会话结束时将其断开。

symmetric cryptographic system(对称密码体制)

一种含有两个变换的密码体制，一个是发方的加密变换，另一个是收方的解密变换。收、发两方使用相同的秘密密钥(或称对称密钥)，或者虽不同，但一种密钥可以很容易地从另一种密钥推导出来。

system integrity(系统完整性)

实现信息系统正常运行及安全保护机制的硬件和软件的完备性时所处的状态。通过系统完整性可衡量计算机系统、数据处理系统或通信系统的硬件与软件的配置是否齐全,逻辑规划和操作是否正确,以及在硬件和软件两个方面是否都得到了可靠、全面、充分的保护形态。

TCB(Trusted Computing Base,可信计算基)

计算机系统内保护装置的总体,包括硬件、固件、软件和负责执行安全策略的组织体。它建立了一个基本的保护环境,并提供一个可信计算机系统所要求的附加用户服务。系统的 TCB 是一个四元组,即[TCB=(M,P,S,O)],其中 M 是软件、硬件与固件的集合,它在存取(访问)控制策略 P 的基础上处理主体集合 S 对客体集合 O 的存取(访问)。

threats(威胁)

威胁是指开发和利用信息系统脆弱性,导致信息系统资源被消耗、欺骗、滥用或运营流程被破坏等,从而对信息系统造成(有意或无意的)危害或不利影响的行为或企图。威胁总是存在的,威胁发生的时间和频度不能被控制。因此,信息安全措施必须被设计成能够阻止或最小化任何针对信息系统的威胁。

training function(培训功能)

在信息系统中,为了充分、有效地进行业务操作、系统维护和应急处置,为了有关员工达到和维持必要的知识和训练水平所必须完成的任务、活动和行动。

Trains Model Framework(培训模型框架)

与角色和责任相关的培训需求、策略、规划、方案和流程的体系性轮廓。

Trojan Horse(特洛伊木马)

具有明显或隐含某种特定功能的计算机程序。它包含了附加的(隐藏的)能暗中利用合法授权的功能,以此达到对信息系统及其资源的未授权操作、窃取、利用或破坏的目的。传说中希腊人打败特洛伊人是凭借一头巨型木马攻入特洛伊城的,因为木马内部藏有武士,但特洛伊人没有识破这一木马计。计算机借用此术语,通常指某些隐含有病毒或恶意功能的程序,看似一个完成正常业务的软件体,实则含有陷阱或攻击程序的通信行为。

TTP(Trusted Third Party,可信任第三方)

在安全策略背景下对某些安全相关活动来说可以信任的安全机构或其代理。

tunnel(隧道)

将一个协议格式的数据包或报文封闭进另一个协议格式的数据包中传输的过程。被封装的协议数据在网络层是不被网络设备识别和处理的,因此类似包过滤防火墙是无法识别和过滤这些协议数据的。

tunneling(隧道技术,隧道效应,隧道结构)

为在运行不同协议的网络之间传递数据包或消息报文而采取的一种传送技术和体系结构,被设计用来提供实现任何标准的点到点封装方案所需要的服务。它可能是一个具有自己特定协议的复杂网络,却可以传递其他网络协议数据。例如通过一个 X.25“隧道”发送 TCP/IP 通信流量,先建立一条 X.25 连接,然后发送 TCP/IP 报文分组,这些报文分组就像数据一样在 X.25 网络中传输。X.25 系统沿连接传递报文分组,并把它们递送到另一个 X.25 端点,在那里再将报文分组提取出来转发到报文分组的目的地。因为隧道技术处理报

文分组如同处理数据一样，因而不考虑该报文的自标识帧。这样，只有当 X.25 的两端事先都同意交换 TCP/IP 报文分组时，这种技术才有效。换而言之，隧道技术是指协议 A 被封装在协议 B 的内部，这样协议 A 就把协议 B 当成是一个数据链路层以通过该链接网络。隧道技术被用来在管理域之间传输数据，这些管理域使用的协议不受连接它们的因特网的支持。在实现任何标准的点到点封装模式时，需要这种网络结构的服务。

Unique Identifier(唯一标识符)

标明身份的不与任何第三方实体属性参数相同的数字或字母符号集合。唯一标识符是指一个代码或一组代码，它们是机构确认个人身份的依据。标识符仅被已指定的实体拥有和使用。

virus(病毒)

在计算机系统中复制自己，把自己与其他程序合并起来，共存于计算机系统中的一种程序。它还可以通过修改其他程序或文件把自己的版本复制到被修改的程序或文件中，从而达到传染的目的。计算机病毒由 3 个部分组成，即病毒引导部分、病毒传染部分和病毒表现(又称破坏)部分。病毒的特点是传染性、潜伏性、隐蔽性和爆发性。

vulnerabilities(脆弱性)

脆弱性是信息系统及组件以及运行环境中的缺陷和漏洞。威胁可能利用脆弱性给信息系统带来危害或不利影响，适当的安全措施可用于减小或消除脆弱性。

WAN(Wide-Area Network，广域网，广域网络)

跨越较大地域范围的一种网络，通常是跨越几十公里到几千公里，甚至全国性的或国际性的网络。与局域网相比，WAN 通常速度慢、延迟大。帧中继、SMDS 和 X.25 都是 WAN 的例子，实际上，因特网是全球最大的广域网。请比较 LAN 和 MAN。

Waste，Fraud and Abuse(损耗、欺骗和滥用)

对系统造成危害的 3 种最基本方式。

Worm(蠕虫)

(网络) 蠕虫是由 Xerox 公司的 Shoch & Hupp 在 ACM 通信(1982 年 3 月)中第一次定义的。它是一种计算机程序，能自我复制并自行传播。蠕虫与病毒不同，它只在网络环境中大量滋生。1988 年 11 月出现的因特网蠕虫可能是最有名的，它成功地覆盖了因特网，在全球 6000 多个网络系统上自我传播。

Zone/Compartmentalization(区域/分隔区)

利用物理和逻辑方法将一个结构完整的区域分离成两个(或以上)具有某种相同属性特征的层次化或类别化的更小一些的区域。

A P P E N D I X B

附录 B 与本书有关的缩略语

AAA	Authentication, Authorization and Accountability	鉴别、权限和可确认性
ACI	Access Control Information	访问控制信息
ACL	Access Control List	访问控制表
ACSE	Association Control Service Element	关联控制服务元素
ADC	ADF Combination	ADF 组合
ADF	Access Control Decision Function	访问控制判决功能
ADI	Access Control Decision Information	访问控制判决信息
AEC	AEF Combination	AEF 组合
AEF	Access Control Enforcement Function	访问控制执行功能
AES	Advanced Encryption Standard	高级加密标准
AH	Authentication Header	鉴别头
AI	Authentication Information	鉴别信息
API	Application Program Interface	应用程序接口
ARP	Address Resolution Protocol	地址解析协议
ASN. 1	Abstract Syntax Notation One	抽象语法表示法 1
ASR	Alternative System Review	备选系统评审
ATM	Asynchronous Transfer Mode	异步传送模式
AUP	Acceptable Use Policy	可接受使用策略
B-ISDN	Broadband-ISDN	宽带 ISDN
BP	Base Practices	基本实施
BSA	Browser-Server-Application	浏览器/服务器应用
C&A	Certification and Accreditation	认证与认可
CA	Certificate Authority	证书机构
CALS	Continuous Acquisition Life-cycle Support	连续获取生命期支持
CC	Common Criteria	通用准则
CCB	Configuration Control Board	配置控制委员会
CCTL	Common Criteria Test Lab	通用准则测试实验室
CDR	Critical Design Review	关键设计评审

CDRL	Contract Data Requirement List	合同数据需求列表
CHAP	Challenge Handshake Authentication Protocol	质询握手鉴别协议
CI	Configuration Item	配置项
CLID	Client ID	客户 ID
CM	Configuration Management	配置管理
CMIS/ CMIP	Common Management Information Service/Common Management Information Protocol	公共管理信息服务/公共管理信息协议
CMISE	Common Management Information Service Element	公共管理信息服务元素
CMM	Capability Maturity Model	能力成熟度模型
CMOL	Common Management Information Protocol Over Logical Link Layer	逻辑链路层上的公共管理信息协议
CMOT	Common Management Information Protocol Over TCP/IP	运行在 TCP/IP 上的公共管理信息协议
CNNIC	China National Network Information Center	中国国家网络信息中心
COEA	Cost and Operational Effectiveness Analysis	成本和运行有效性分析
COMPUSEC	Computer security	计算机安全
CONOP	CONcept of OPeration	(客户的)操作概念
COS	Class Of Service	服务类型
CSCI	Computer Software Configuration Item	计算机软件配置项
CWBS	Contract Work Breakdown Structure	合同工作细目分类结构
DAA	Designated Approving Authority	指定批准机构
DBMS	Database Management System	数据库管理系统
DES	Data Encryption Standard	[美]数据加密标准
DESE	DES Encryption	(微软)加密(协议)
DH	Diffie-Hellman	Diffie-Hellman(公开密码算法)
DID	Data Item Description	数据项描述
DNS	Domain Name System	域名系统
DOI	Domain of Interpretation	解释域
DS	Digital Signature	数字签名
DT&E	Development Test and Evaluation	开发测试和评估
DTE	Data Terminal Equipment	数据终端设备
DTS	Data Tracking Sheet	数据跟踪表(单)
EAL	Evaluation Assurance Level	评估保证级
ECP	Encryption Control Protocol	加密控制协议
EDI	Electronic Data Interchange	电子数据交换
E-Mail	Electronic Mail	电子邮(函)件
ESP	Encapsulation Security Payload	封装安全载荷
ESR	Evaluation Summarization Report	评估总结报告
ETR	Evaluation Technology Report	评估技术报告
FBI	Federal Bureau of Investigation	[美]国家联邦调查局
FCA	Functional Configuration Audit	功能配置审计
FDDI	Fiber Distributed Data Interface	分布式光纤数据接口
FDMA	Frequency Division Multiple Access	频分多址访问(存取)
FHSS	Frequency Hopped Spread Spectrum	跳频扩展频谱技术

GMITS	Guidelines for the management of IT security	IT 安全管理指南
GP	Generic Practices	通用实施
HCI	Hiding Confidentiality Information	隐藏机密性(的)信息
HDLC	High-level Data Link Control	高级数据链路控制
HGW	Home Gateway	总部网关
IATF	Information Assurance Technical Framework	信息保障技术框架
ICMP	Internet Control Message Protocol	互联网控制消息协议，因特网控制消息协议
ICV	Integrity Check Value	完整性校验值
ID	Identification	识别
ILS	Integrated Logistics Support	一体化的后勤支持/综合的后勤支持
INFOSEC	INFOrmation system SECurity	信息系统安全
IOC	Initial Operational Capability	初始运行能力，初始操作能力
IP	Internet Protocol	互联网协议
IPCP	IP Control Protocol	IP 控制协议
IPOA	IP Over ATM	ATM 上的 IP
IPSec	IP Security	IP(层)安全(协议)
ISAKMP	Internet Security Association and Key Management Protocol	因特网安全关联和密钥管理协议
ISMS	Information Security Management System	信息安全管理体系
ISO	International Standard Organization	国际标准化组织
ISP	Internet Service Provider	因特网服务供应商
ISSE	Information System Security Engineering	信息系统安全工程
IT	Information Technology	信息技术
ITSEC	Information Technology Security Evaluation Criteria	信息技术安全评估准则
IV&V	Independent Verification and Validation	独立验证和证实
KDC	Key Distribution Center	密钥分发中心
KMI	Key Management Infrastructure	密钥管理基础设施
KTC	Key Translation Center	密钥转移中心
LAN	Local Area Network	局域网
LCIE	Life-Cycle INFOSEC Engineering	生命期信息系统安全工程
MAC	Medium Access Control	介质访问控制
MAC	Mandatory Access Control	强制访问控制
MAC	Message Authentication Code	消息鉴别码
MAN	Metropolitan Area Network	城域网
MIB	Management Information Base	管理信息库
MIC	Message Integrity Code	消息完整性编码
MID	Multiplexing ID	复用 ID
MISSI	Multilevel Information Systems Security Initiative	多级信息系统安全倡议
MK	Master Key	主密钥
MNS	Mission(Capability)Needs Statement	任务(能力)要求说明
MPPE	Microsoft Point To Point Encryption	(微软)点到点加密(协议)
MVLAN	Main VLAN	主虚拟局域网

NAS	Network Access Server	网络访问服务器
NAT	Network Address Translation	网络地址转换
NCP	Network Control Protocol	网络控制协议
NII	National Information Infrastructure	国家信息基础设施
N-ISDN	Narrow-ISDN	窄带 ISDN
NOS	Network Operating System	网络操作系统
NR-TTP	Non-repudiation-TTP	抗抵赖可信第三方
OA	Office Automation	办公自动化
OAN	Operation Area Network	操作域网,运行域网
ODP	Open Distributed Processing	开放分布式处理
OID	Object identifier	对象(客体)标识符
OPM	Office of the Personal Management	人事管理办公室
ORD	Operational Requirements Document	运行需求文档,操作需求文档
OSA	Open System Architecture	开放系统体系结构
OSI	Open System Interconnection	开放系统互连
OSI/RM	OSI Reference Model	OSI 参考模型
OSIE	OSI Environments	开放系统互连环境
OT&E	Operational Test and Evaluation	操作测试与评估,运行测试与评估
P3I	Pre-Planned Product Improvement	预(先)计划的产品改进
PA	Process Area	过程区
PC	Personal Computer	个人计算机
PCA	Physical Configuration Audit	物理配置审计
PDCA	Plan,Do,Check and Act	规划、实施、检查和改进(模型),PDCA 模型
PDR	Preliminary Design Review	初级设计评审
PDU	Protocol Data Unit	协议数据单元
PIN	Personal Identification Number	个人标识号,个人身份号
PKI	Public Key Infrastructure	公开密钥基础设施
PM	Program Manager	程序管理员
PMI	Privilege Management Infrastructure	授权/权限管理基础设施
PMO	Program Management Office	项目管理办公室
PMP	Program Management Plan	项目管理计划
PP	Protection Profile	保护轮廓
PPP	Point To Point Protocol	点到点协议
PPTP	Point To Point Tunneling Protocol	点到点隧道协议
PVG	patch and vulnerability group	补丁和脆弱性(处理)组
PWBS	Program Work Breakdown Structure	项目工作分类结构
QoS	Quality of Service	服务质量
RAA	(Security) Risk Acceptance Authority	(安全)风险验收(权威)机构
RADIUS	Remote Authentication Dial-In User Service	远程鉴别拨入用户服务
RBAC	Role-Based Access Control	基于角色的访问控制
ROSE	Remote Operations Service Element	远程操作服务元素
SAPI	Security Application Program Interface	安全应用程序接口
SDA	Security Domain Authority	安全域机构

SDNS	Secure Data Network System	安全数据网系统
SDU	Service Data Unit	服务数据单元
SE	System Engineering	系统工程
SE-CMM	Systems Engineering Capability Maturity Model	系统工程能力成熟度模型
SEDS	System Engineering Detailed Schedule	系统工程详细进度表
SEMP	System Engineering Management Plan	系统工程管理计划
SEMS	System Engineering Main Schedule	系统工程主进度表
SF	Security Function	安全功能
SFA	Security Fault Analysis	安全故障分析
SFP	Security Function Policy	安全功能策略
SFR	System Functional Review	系统功能评审
SI	Security Information	安全信息
SMIB	Security Management Information Base	安全管理信息库
SNA	System Network Architecture	系统网络体系结构
SNMP	Simple Network Management Protocol	简单网络管理协议
SOF	Strength of Function	功能强度
SOW	Statement of Work	工作说明,工作陈述
SP	Service Provider	服务供应商
SPD	Security Policy Database	安全策略数据库
SPI	Security Parameter Index	安全参数索引
SPO	System Program Office	系统项目办公室
SQL	Structured Query Language	结构化查询语言
SRM	Security Risk Management	安全风险管理
SRR	System Requirement Review	系统需求评审
SSAM	Systems Security Engineering Capability Maturity Model (SSE-CMM) Appraisal Method	系统安全工程能力成熟度模型评估方法
SSE	Systems Security Engineering	系统安全工程
SSE-CMM	Systems Security Engineering Capability Maturity Model	系统安全工程能力成熟度模型
SSR	Software Specification Review	软件规范评审
ST	Security Target	安全目标
STAR	System Threat Assessment Report	系统威胁评估报告
STDM	Statistical Time Division Multiplexing	统计时分复用(技术)
SVR	Security Verification Review	安全验证评审
TAFIM	Technical Architecture Framework for Information Management	信息管理的技术体系结构框架
TCP	Transmission Control Protocol	传输控制协议
TCSEC	Trusted Computer System Evaluation Criteria	可信计算机系统评估准则
TEMPEST	Transient ElectroMagnetic Pulse Emanation STandard, Telecommunications Electronics Material Protected from Emanating Spurious Transmissions	瞬态电磁脉冲辐射[标准],防电磁泄露[技术]
TNG	Trusted Network Guideline	可信网络指南
TOE	Target of Evaluation	评估对象
TPM	Technical Performance Measurement	技术性能测量

TRR	Test Ready Review	测试准备就绪评审
TSC	TSF Scope of control	评估对象安全功能控制范围，TSF 控制范围
TSDM	Trusted Software Development Methodology	可信软件开发方法学
TSF	TOE Security Function	评估对象安全功能，TOE 安全功能
TSFI	TSF Interface	评估对象安全功能接口，TSF 接口
TSP	TOE Security Policy	评估对象安全策略，TOE 安全策略
TSP	Telecommunication Service Provider	通信服务供应商
TTP	Trusted Third Party	可信第三方
V&V	Verification & Validation	验证与证实
VPN	Virtual Private Network	虚拟专(用)网
WAN	Wide Area Network	广域网
WWW	World Wide Web	万维网

参 考 文 献

[1] (中办发[2003]27 号)文件,《国家信息化领导小组关于加强信息安全保障工作的意见》,2003 年 7 月 9 日.

[2] (公通字[2007]43 号),信息安全等级保护管理办法.公安部、国家保密局、国家密码管理局、国务院信息化工作办公室.2007 年 6 月 22 日.

[3] 戴宗坤,罗万伯,等.信息系统安全.北京:电子工业出版社.2002.

[4] 戴宗坤,罗万伯,刘嘉勇,等.信息安全法律法规与管理.重庆:重庆大学出版社.2005.

[5] 戴宗坤,罗万伯,胡勇,等.信息安全管理指南.重庆:重庆大学出版社. 2008.

[6] ISO/IEC 13335-1:2004. Information Technology — Security Techniques — Management of Information and Communications Technology Security — Part 1: Concepts and Models for Information and Communications Technology Security Management[S].

[7] ISO/IEC 13335-2. Information Technology—Guidelines for the Management of IT Security —Part 2: Managing and Planning IT Security (2nd WD) [S].

[8] ISO/IEC TR 13335-3:1998. Information Technology — Guidelines for the Management of IT Security — Part 3: Techniques for the Management of IT Security[S].

[9] ISO/IEC TR 13335-4:2000. Information Technology — Guidelines for the Management of IT Security — Part 4: Selection of Safeguards[S].

[10] ISO/IEC TR 13335-5:2001. Information Technology — Guidelines for the Management of IT Security — Part 5: Management Guidance on Network Security[S].

[11] ISO/TR 13569:2005. Financial Services — Information Security Guidelines[S].

[12] ISO/IEC 15408-1:2005. Information Technology — Security Techniques — Evaluation Criteria for IT Security — Part 1: Introduction and General Model[S].

[13] ISO/IEC 15408-2:2005. Information Technology — Security Techniques — Evaluation Criteria for IT Security — Part 2: Security functional Requirements[S].

[14] ISO/IEC 15408-3:2005. Information Technology — Security Techniques — Evaluation Criteria for IT Security — Part 3: Security Assurance Requirements[S].

[15] ISO/IEC TR 15443-1:2005. Information Technology — Security Techniques — A Framework for IT Security Assurance — Part 1: Overview and Framework[S].

[16] ISO/IEC TR 15443-2:2005. Information Technology — Security Techniques — A Framework for IT Security Assurance — Part 2: Assurance Methods[S].

[17] ISO/IEC 17799:2005. Information Technology — Security Techniques — Code of Practice for Information Security Management[S].

[18] ISO/IEC 18028-2:2006. Information Technology — Security Techniques — IT Network Security — Part 2: Network Security Architecture[S].

[19] ISO/IEC 18028-3:2005. Information Technology — Security Techniques — IT Network Security — Part 3: Securing Communications Between Networks Using Security Gateways[S].

[20] ISO/IEC 18028-4:2005. Information Technology — Security Techniques — IT Network Security — Part 4: Securing Remote Access[S].

[21] ISO/IEC TR 18044:2004. Information Technology — Security Techniques — Information Security Incident Management[S].

[22] ISO/IEC TR 19791:2006. Information Technology — Security Techniques — Security Assessment of Operational Systems[S].

[23] ISO/IEC 27001:2005. Information Technology — Security Techniques — Information Security

Management Systems — Requirements[S].

[24] GB/T 9387.2—1995.信息处理系统 开放系统互连 基本参考模型 第2部分：安全体系结构(idt ISO 7498-2)[S].

[25] GB/T 9387.4—1995.信息处理系统 开放系统互连 基本参考模型 第4部分：安全管理框架(idt ISO 7498-4)[S].

[26] GB/T 17142—1997.系统管理综述(Systems Management Overview)(idt ISO/IEC 10040 (CCITT X.701))[S].

[27] GB 17859—1999.计算机信息系统安全保护等级划分准则[S].

[28] 戴宗坤,等.英汉网络与信息安全辞典.北京：电子工业出版社. 2004.

[29] ISO/IEC TR 14516：2002. Information Technology — Security Techniques — Guidelines for the Use and Management of Trusted Third Party[S].